2008

What Makes Them Click? Applying The Rational Choice Perspective To The Hacking Underground

Michael Bachmann
University of Central Florida

WHAT MAKES THEM CLICK?
APPLYING THE RATIONAL CHOICE PERSPECTIVE
TO THE HACKING UNDERGROUND

by

MICHAEL BACHMANN
M.A. University of Mannheim, 2004

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in the Department of Sociology
in the College of Sciences
at the University of Central Florida
Orlando, Florida

Summer Term
2008

Major Professor: Jay Corzine

ABSTRACT

The increasing dependence of modern societies, industries, and individuals on information technology and computer networks renders them ever more vulnerable to attacks on critical IT infrastructures. While the societal threat posed by hackers and other types of cyber-criminals has been growing significantly in the last decade, mainstream criminology has only recently begun to realize the significance of this threat. Cyber-criminology is slowly emerging as a subfield of criminological study and has yet to overcome many of the problems other areas of criminological research have already mastered. Aside from substantial methodological and theoretical problems, cyber-criminology currently also suffers from the scarcity of available data. As a result, scientific answers to crucial questions, such as who exactly the attackers are and why they engage in hacking activities, remain largely fragmentary.

The present study begins to fill this remaining gap in the literature. It examines survey data about hackers, their involvement in hacking, their motivations to hack, and their hacking careers. The data for this study was collected during a large hacking convention in Washington D.C. in February 2008. The theoretical framework guiding the analyses is the rational choice perspective (Clarke & Cornish, 1985). Several hypotheses about hackers are derived from the theory and some of its models are transposed into the context of hackers. Results suggest that the rational choice perspective is a viable theory when applied to cyber-criminals. Findings also demonstrate that the creation of more effective countermeasures requires adjustments to our understanding of who hackers really are and why they hack.

To my wife and family, who of all that walk the earth, are most precious to me and whose continuing support and love enabled me to write this dissertation.

ACKNOWLEDGMENTS

I would like to deeply thank some of the persons who, during the several months of this endeavor, provided me with the necessary support and helpful assistance. Without their care and consideration, this dissertation would not have matured in the same way.

In particular, I would like to thank the members of my dissertation committee for their encouragement, guidance, and their feedback during all phases of this project. One of my wisest decisions as student was to select Dr. Jay Corzine as my dissertation chair. He was an excellent and committed supervisor of this project, and he also proved to be an invaluable help during my job search. I would further like to thank him as well as Dr. Jana Jasinski and Dr. James Wright (in alphabetical order) for providing me with the opportunity to even become a Ph.D. student at University of Central Florida, and to do so at a unique moment in time—during the start of a new program. All of them provided me with an excellent education that significantly altered my life-course trajectory and turned me into the person I am today. I would further like to extend my gratitude to my external committee member Dr. John Jarvis, whose contacts and expertise were exceptionally helpful for this project.

Second, I would like to especially thank my colleague Dr. Monica Mendez for her offer to review and edit my drafts. Without her nuanced understanding of English language, this dissertation would not have been written in the same way. I cherish the time we spent together and hope we will be able to stay in touch despite the large distance that will be between us.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS/ABBREVIATIONS

ARPANET	Advanced Research Projects Agency Network
BJS	Bureau of Justice Statistics
CGI	Common Gateway Interface
CMC	Computer-mediated communication
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
DOJ	U.S. Department of Justice
EFA	Exploratory Factor Analysis
ICMP	Internet Control Message Protocol
I2P	Invisible Internet Project
IP	Internet Protocol
IRB	Institutional Review Board
IT	Information Technology
NCSS	National Computer Security Survey
NCSD	National Cyber Security Division (U.S. Department of Homeland Security)
NIBRS	National Incident Based Reporting System
OS	Operation System
P2P	Peer-to-peer network
PDP	Programmed Data Processor
REI	Rational-Experiential Inventory
RPC	Remote Procedure Calls

TCP	Transmission Control Protocol
TOR	The Onion Router
UCR	Uniform Crime Report
UDP	User Datagram Protocol
UNIX	UNiplexed Information and Computing System
URL	Uniform Resource Locator

New technologies do not determine the particulars of human fates;
they alter the spectrum of potentialities within which
people may act (McClintock, 1999, p. 3)

CHAPTER ONE:
INTRODUCTION

Estonia, April 26, 2007. In retaliation for the removal of a World War II-era statue of a Soviet soldier, pro-Russian hackers launched a month-long campaign that has become known as the first war in cyberspace. Using a technique known as distributed denial-of-service attack (DDoS) on a hitherto-unprecedented scale, the attackers managed to effectively shut down vital parts of Estonia's digital infrastructures. In a coordinated effort, an estimated one million remote-controlled computers from around the world were used to bombard the Web sites of the president, the prime minister, Parliament and other government agencies, Estonia's biggest bank, and several national newspapers with requests. The attacks were so massive that NATO rushed a cyber-warfare team of international security experts to assist the Estonian government, and the country's defense minister, Jaak Aaviksoo, who described the attack as a national security situation, requested that the European Union classify it as an act of terrorism (Landler & Markoff, 2007). In reference to the events in Estonia, Suleyman Anil, the head of NATO's incident response center, later warned attendees of the 2008 E-Crime Congress in London that "cyber defense is now mentioned at the highest level along

with missile defense and energy security." According to Anil, "we have seen more of these attacks and we don't think this problem will disappear soon. Unless globally supported measures are taken, it can become a global problem" (Johnson, 2008, p. 1).

Turkey, May 18, 2006. A Turkish hacker who calls himself 'iSKORPiTX' commits the biggest hacking incident in web-hosting history. He successfully hacked and defaced at least 21,549 websites simultaneously and another 17,000 websites a few hours later (Lemos, 2006). For the time being, this incident marks the largest single defacement attack in the fast growing area of website hackings, but it is merely one of many cases. According to Zone-H, the Internet's watchdog on website defacements, iSKORPiTX alone has defaced close to 189,000 websites, and the top 50 attackers hacked a total of approximately 2.5 million websites across the globe (Zone-H, 2007). These numbers are supported by the exponential increase in website defacements found in the CSI/FBI Computer Crime and Security Survey (2005). In 2004, 5% of the respondents experienced 10 or more website incidents, while in 2005 that figure went up to 95% (L. A. Gordon, Loeb, Lucyshyn, & Richardson, 2005).

The above examples are merely two incidents of what have become a long series of high-profile hacking attacks (Aguila, 2008). Although warnings of the societal threat posed by cyber-attacks on critical network infrastructures have been heralded since the 1980s, it is only in recent years that the problem has made it onto the radar of governments. Partly due to the experiences of Estonia, countries around the globe are now reassessing the security situation of their key information systems. They are enacting new security measures to better protect their critical network infrastructures, and they are increasing their readiness to respond to large-scale computer incidents

(NCIRC, 2008). In Britain, for example, Conservatives have recently proposed the creation of a new position for a cyber-security minister and a national hi-tech crimes police squad to better combat the “growing and serious threat to individuals, business and government […] that will continue to escalate as technology changes” (Johnston, 2008, p. 1).

The implementation of effective countermeasures against hacking attacks is exceedingly facilitated by the vast amount of knowledge that has already been accumulated in numerous computer science research projects (cf. Chirillo, 2001; Curran et al., 2005; J. Erickson, 2008). Several studies conducted by computer scientists and computer engineers have closely examined the technical details of the various attack methods and have produced a significant body of information that can now be applied to help protect network infrastructures (Casey, 2004). Unfortunately, the guidance provided by these studies is limited to only the technical aspects of hacking attacks and, sharply contrasting from the substantial amount of knowledge already gathered about how the attacks are performed, answers to the questions of who exactly the attackers are and why they engage in hacking activities continue to remain largely speculative. Today, the persons committing the attacks remain mysterious for the most part, and scientific information about them continues to be only fragmentary.

The present lack of information concerning the sociodemographic characteristics and the motives of cybercrime offenders can be attributed to a number of causes. One of the main reasons can be traced back to the unfortunate circumstance that, until recently, mainstream criminology has underestimated the potentially devastating societal impacts of cybercrimes and has diverted only limited attention to this relatively new type

of criminal behavior (Jaishankar, 2007; Jewkes, 2006; Mann & Sutton, 1998). Cyber-criminology is only now beginning to evolve as a distinct field of criminological research, and it has yet to overcome many methodological and theoretical problems that other areas of criminological research have already solved (Yar, 2005b, 2006).

A particular challenge for researchers in this young field of study arises from the various methodological obstacles entailed in the sampling of cyber-criminals. As a result of these difficulties, available data sources are scarce, and quantitative studies are limited to surveys of cybercrime victims. At this point, only a few qualitative case studies (eg. Mitnick & Simon, 2005; Schell, Dodge, & Moutsatsos, 2002; Taylor, 1999, 2000) and biographies (eg. Mitnick, Simon, & Wozniak, 2002; Nuwere & Chanoff, 2003) exist that examine individual hackers, their motivations, preferences, and their hacking careers. While such studies are well suited to provide in-depth insights into the lives of a few individuals, they are unfit for generating generalizable information about the population of hackers at large. Yet, just “like in traditional crimes, it’s important to try to understand what motivates these people to get involved in computer crimes in the first place, how they choose their targets and what keeps them in this deviant behavior after the first initial thrill” (Bednarz, 2004, p. 1). This comment, stated by Marcus Rogers, an associate professor at Purdue University and head of the cyber-forensics research in the department of computer technology, accurately describes the task cyber-criminologists have to accomplish. The aim of the present study is to undertake this task and to begin filling the remaining gap in the criminological literature on hackers and the hacking community by providing the first quantifiable insights into the hacking underground. Such insights are needed to create a more profound understanding of the nature of the

threat and a more complete assessment of the problem and its solutions. The identification of the reasons and motives for an attack helps to better identify the actors' behaviors, to develop better countermeasures, and to ultimately make systems safer. To accomplish this goal, the study is structured as followed.

First, a detailed introduction into the fiercely contested dispute over the definitions of the terms "hacker" and "hacking" is provided, and the exact usage of both terms in the study is specified. Second, the typical perceptions of hackers in the general public are discussed. Most people do not have direct contacts with hackers, but derive their knowledge of the hacking scene and the digital underground from mass media or stereotype-laden, personal prejudices. Unveiling the common (mis)perceptions about hackers is an important part of the present study because a clear, scientific vision of the characteristics of the hacking community has to be established against the context of the predominant perceptions of who hackers are and why they hack.

Third, the present study is located within the current state of cyber-criminology. The developments that have led to the establishment of cyber-criminology as a distinct field within criminological research are traced, and the justifications for this establishment are discussed. Then, detailed descriptions are provided of the current methodological and theoretical challenges with which cyber-criminologists are confronted. When studying hacking activities, it is important to bear in mind that hacking is a form of cybercriminal activity, and, as such, it is subjected to the various obstacles challenging all studies of criminal activities that are taking place in the virtual worlds of interconnected computer networks.

Fourth, the theoretical framework guiding the study is introduced. The study follows the rational choice perspective (Clarke & Cornish, 1985), a popular criminological version of rational choice theory. A rationale for the selection of this particular theoretical framework is provided and its core components are discussed. The central hypotheses of the study are derived from the main propositions of the rational choice perspective, and Clarke and Cornish's (1985) central models of the decision-making processes are modified to fit the context of hackers.

Following the introduction of the theoretical framework, the details of the research design are specified. A rationale for the selection of a particular sampling strategy is provided, and the steps involved in the processes of creating the survey instrument and collecting the data are elaborated. The discussion of the various aspects of the research design is concluded by a separate chapter on the different sections and individual items of the survey instrument.

The last two chapters of this study present and discuss the findings of the research project. The results paint a detailed picture of distributions of a range of sociodemographic characteristics within the hacking community. They further specify the relative importance of various motivations, and they assess several components of the suggested theoretical frameworks. The study concludes with a discussion of the implications these findings hold for our understanding of who hackers are and why they hack, for the design of more effective countermeasures, and for the appropriateness of the rational choice perspective as a theoretical framework for the study of computer hackers. The limitations of the current project are considered and suggestions for future research are given.

CHAPTER TWO:
THE MEANINGS OF HACKING AND HACKERS

An indispensable step in every scientific research project is the explicit operationalization of the main study concepts. The first important step within this process is the specification of central terms and core concepts with precise definitions. In the context of hackers, this step is of crucial importance. Devising exact definitions of the terms hacker and hacking is particularly problematic because both terms are fiercely contested within the hacking community itself and between hackers and the general public. Thus, a description of the various meanings ascribed to both terms is necessary for a complete understanding of the various definitions and the disputes between them.

The Controversial Meanings of Hacker and Hacking

Applied to the context of computer technology, the two terms “hacker” and “hacking” were originally used only in small circles of computer experts, and familiarity with both terms was limited to a few specialized computer scene insiders. The popularity of the two terms slowly began to increase during the late 1980s and 1990s, when they became more commonly adopted in mainstream media reports of several high-profile cyber-trespasses that sometimes involved shocking exploitations of computer and telecommunication technologies (cf. Aguila, 2008). In recent years, the more frequent media coverage of such computer abuses has turned these formerly uncommon terms into the everyday vernacular of the mainstream public discourse (K. Erickson & Howard, 2007; Schell & Martin, 2004).

Today, the vast majority of the general population has at least some vague idea about what hackers are and what they do. The typical understanding of a hacker is that of a perpetrator who illegally invades other people's computer systems with the intent to destroy, disrupt, or carry out illegal activities on that system. As Taylor notes in his prominent study on hackers and the hacking community, the public perceives hacking as "the unauthorized access and subsequent use of other people's computer systems" (Taylor, 1999, p. xi). Unfamiliar with the specific details of hacking, many members of the general public even tend to imprecisely subsume any illegal abuse of a computer system or network under the term hacking. This inaccurate perception of hackers is hardly surprising because hackers and hacking have become the center of present-day public debates about cybercrimes. In fact, mainstream media reports oftentimes use the terms hacker and hacking synonymously with cyber-criminals and cybercrimes (K. Erickson & Howard, 2007; Yar, 2005a). Moreover, most media coverage of hackers tends to reinforce their stereotypical perception as prototypes of mysterious and dangerous cyber-criminals. As a result, hackers are commonly seen as personified representations of the threat cybercrimes pose to society (K. Erickson & Howard, 2007).

This common conceptualization of hackers and their activities, while unanimously accepted and unchallenged within the public discourse, is actually deceptive because it oversimplifies the meaning of hackers and hacking in a twofold way: It overlooks the vicissitudinous etymological history of the two terms, and it ignores that both terms remain deeply contested today. To familiarize the reader with the historical and contemporary controversies surrounding the meanings and connotations of hackers and hacking, both aspects are discussed in the following section.

The Etymological History of the Term Hacker

Since its first appearance in Yiddish language, where it was used to denote someone as inept as to make furniture with an axe (Schell & Martin, 2004), the term "hacker" has undergone many changes. According to the Oxford English Dictionary (2008), the first emergence of the term in English language dates back to 1480, when it was used to signify a tool used for hacking, chopping wood, or breaking up the earth. A century later, the first reference to a "hacker" as a person was recorded in English language. Back then, the word was used to identify someone as a cutter, a cut-throat, a notorious thief, or generally as a bully or a rogue. This meaning was again slightly changed about 30 years later, when Thomas Cartwright (1618) used the term as a characterization of somebody who mangles words, senses, and meanings. Around the same time this shift in meaning took place, a second, completely different connotation of the word "hacker" emerged. This new version signified a farm laborer who hacks or cuts more than half an acre of ground in a day with a hack (Oxford English Dictionary, 2008). The etymological history of the term "hacker," especially the double entendre that existed during the 17th century where it referred to both malevolent outlaws and persons who excelled in their legitimate profession, is particularly interesting because both connotations have again resurfaced in the contemporary debate surrounding the meaning of the word.

After it had almost fallen into oblivion in intervening years, the term "hacker" resurfaced again in the context of computer technology during the 1960s. It was reintroduced as a neologism into the specialized and confined language of computer techni-

cians and programming experts, who used it as a positive label for somebody who was particularly skilled in developing highly efficient, creative, and compact programs and algorithms. Rather than simply using existing computer technology, “hacker” enthusiasts were united in their passion for technological innovations and by their playful and individualistic quest to satisfy their intellectual curiosity. “Hacker” in this understanding denotes someone who is obsessed with designing computer software and hardware, a superb technician who possesses a substantial degree of skill and competence and spends much of his time writing computer programs. Respectively, “hacking” originally referred to the continuous improvement of computer program codes and algorithms, of software applications and hardware components.

It was hackers who first realized the true potential behind the steel facades of computing machines which—as a side note—were originally developed to better calculate the trajectories of ballistic projectiles. Among the many inventions attributed to hackers are, for example, the first computer chess applications and even the Apple computer, one of the first personal computers (Schrutzki, 1989, p. 166). All early contributors to the advancement and expansion of computer technology, all innovators who developed new computer-based solutions to a multitude of problems, all entrepreneurs who pioneered and fostered the “computer revolution” (Naughton, 2000, p. 313), and all those who paved the way for today’s superhighways of the Internet, were considered prototypical hackers in this original understanding of the term (Levy, 1984).

The original hacker community formed a subculture shaped by the ideals and moral concepts of the zeitgeist. As did many other sub- and counterculture movements at the time, the early hacking community was characterized by a fundamental distrust

against governmental and military monopolies, power, and authority. Early hackers defied corporate domination of culture and rejected traditional and conservative values, norms, and lifestyles. Instead, they genuinely adhered to the enlightenment ideals of human emancipation and self-fulfillment through rational thought. They advocated the freedom of information, knowledge, and intellectual thought, and promoted the idea that information and knowledge should be accessible for everyone without restrictions (Thomas, 2002). Many members of the hacking community were idealists who advertised the usage of computer technology for the higher goals of intellectual discovery, for creating art, beauty, and for improving the overall quality of life (Schrutzki, 1989). Still today, programming and other activities that support these views are oftentimes referred to as “hacktivism” within the hacking subculture to emphasize their political nature (Taylor, 2004).

While their exploratory quests for new information and data frequently included unauthorized accesses to remote computer systems, traditional hackers undertook such accesses without criminal intent. Instead, they were carried out to investigate and better understand the intricacies of different system setups, to utilize existing computing resources (which at the time were very costly), to detect security breaches and weaknesses, and to ultimately enhance the security of computer protections. The vast majority of members of the original hacker community adhered to a “Hacker Ethic,” a set of rules that was introduced by Steven Levy (1984) to describe the values of the hackers at the MIT Artificial Intelligence Laboratory. The main principles of this Hacker Ethic are that: 1) access to computers and anything which might teach something about how the world works should be unlimited and total; 2) all information should be free; 3) authority

should be mistrusted and decentralization promoted; 4) hackers should be judged solely by their hacking, not ascribed criteria such as degrees, age, race, or position; 5) art and beauty can be created on a computer; and 6) computers can change life for the better (Levy, 1984). One important implication of this Ethic is that any form of damage to remote computer systems, be it intentional or as a result of incompetence, is principally objectionable and contemptible.

The Current Controversy Over the Meaning of Hacker

As was mentioned earlier, the original positive meanings of the terms hackers and hacking became gradually substituted with negative connotations in the 1980s and 1990s. The increasingly mission-critical nature of computer networks for many industries and the expanding popularity of electronic financial transactions began to interest many people in breaking into computer systems, not in an attempt to understand them or make them more secure, but to abuse, disrupt, sabotage, and exploit them. Angered by what from their perspective appeared to be a misrepresentation and a denunciation of the hacking community, traditional hackers reacted to this development by introducing the new label “crackers” for unethical and menacing hackers, from whom they attempted to distinguish themselves. It is important to note that in the context of the debate about hackers, the term “crackers” has no racist connotation. Rather, it is derived from the activity of cracking, or breaking into, a safe and it refers to people who breach (or crack) security measures on a computer system, a network, or an application with the intent to damage or exploit the target or to steal information from it. Hackers who engage in these kind of malicious activities and for whom the label “cracker” was in-

tended, on the other hand, largely reject it because cracking typically involves programming software applications specifically designed to discover and exploit weaknesses. In their logic, the ability to create programs that are able to circumvent or breach defensive security measures is proof of their ability to write superior code. Hence, they prefer to refer to themselves as hackers.

The fiercely contested battle over these two labels created considerable linguistic confusion. Making matters even worse, however, is the circumstance that the distinction between hackers and crackers is not the only controversial differentiation. Similar to the distinction that exists between “hackers” and “crackers,” and just as contested, is the differentiation between “white hat” and “black hat” hackers. Again, these two terms do not have a racist background, but are derived from old black-and-white western movies, in which the sinister villain typically wore a black hat, and his law-abiding or law-enforcing counterpart a white hat. Applied within the context of computer technology, “white hat” denotes hackers who abide by the Hacker Ethic and hold its rules in highest regard, whereas “black hat” hackers do not commit themselves to the same ethical standards.

Today, white hat hackers are oftentimes employed or contracted by computer companies, governments, and financial institutions. Their job is to identify security weaknesses and holes in computer systems, networks, or newly-developed software applications and hardware components. Ethical hacking, or “penetration testing,” emerged as a byproduct of the increasing need for all corporations, organizations, and social institutions to be permanently connected to the Internet. In an attempt to avoid being victimized by black hat hackers, many corporations and agencies decided to hire

or contract white hat hackers, who secure their networks by legally attempting to break into them (Damsell, 2003).

Whereas many penetration testers practice ethical hacking as a legal profession, the term “ethical hacker” remains an oxymoron for many black hat hackers. For them, true hacking implies compromising the security of a system without permission from an authorized party. Although there continues to be a controversy over when the term black hat was coined and to whom it was first applied, many reports identify John Draper (a.k.a. Captain Crunch) as the first cracker to whom the label black hat hacker was applied, even though he was de facto a phreaker, a person who hacks telephone systems (Schlegel & Cohen, 2007). Draper used a plastic whistle from a cereal box to generate the exact 2,600 Hz tone American Telephone and Telegraph (AT&T) and other telephone providers used at the time to indicate the availability of long-distance phone lines. By mimicking the whistling of a dial tone, Draper tricked the controlling connection switch into stopping all billing because the switch assumed the call had ended. With the help of their cereal box whistles, Draper and his friends could call each other for free—at least until irregularities in the account billing were discovered and Draper was sentenced to prison (Schell & Martin, 2004).

Draper and his friends are just one example of the countless young, creative crackers who experiment with security mechanisms in an attempt to break them and who learn from each other in the computer underground. While the majority of hackers, especially the masses of unskilled “script kiddies,” who merely download and execute preconfigured attack applications and routines, can adequately be subsumed under the label of black hat hackers (Twist, 2003), the contested nature of the terms “hacker” and

“hacking” within the scene is important to bear in mind when studying hackers. Studies that do not distinguish between white hat penetration testers and criminal black hat hackers will inevitably introduce a bias that produces distorted and inaccurate results.

Notwithstanding the resistance to the criminal label within the traditional hacker community, large parts of the general public are either unaware or ignorant of the distinctions between hackers and crackers, white hats and black hats. Similarly, the mainstream media as well as law enforcement agencies and computer security industries generally do not subscribe to these distinctions. Instead, they subsume any type of hacking activity under the currently predominant definition as an inherently negative, criminal activity. They usually also equate hackers with cyber-criminals, merely because this is how the vast majority of people outside of the community understand hacking and hackers (Twist, 2003). Thus, the definitions of what constitutes a hacker and hacking activities are not only deeply contested within the hacking underground, but also between the general public and the members of the hacking community, to whom the criminal label is universally applied. While many black hat hackers accept or embrace this label, self-proclaimed white hat hackers consider themselves misrepresented by it and continue to challenge and reject the label.

Although the above section shows that awareness of the different meanings associated with the two terms “hacker” and “hacking” and of their contested nature is important for the study of hackers, subsequent uses of both terms will refer to the understanding shared in the general public. This usage is not intended to discriminate against traditional hackers or penetration testers, but has a twofold reason. First, the focus of

this study lies solely on illegal hacking activities. The second reason is simply pragmatic brevity.

The (Mis)representations of Hackers in the General Media

While hacking as the unauthorized intrusion into computer systems with the intent to abuse or exploit them is undoubtedly at the center of commonly held stereotypes about hackers, their conventional representations are far more complex. They involve several additional assumptions, many of which are problematic because they are stereotypical misrepresentations (Thomas, 2002). The distorted picture of hackers is partly a result of the circumstance that only very few people have direct personal contacts to actual hackers in their social networks. Without direct personal experience, the vast majority of people derive their knowledge about hackers from representations in popular fiction and the media. Thus, an examination of popular hacker representations has to proceed from reviewing their depiction in mainstream media and culture.

The representation of hackers in the general media can be best understood against the wider context of societal responses to technological innovations and transformations (Taylor, 1999, 2000). In the past, many such transformations have provoked both technophobic fears and technophilic fascinations in equal measures. Historically, the introduction of any new technology with the potential to transform social structures and interactions has routinely created a tension between an anticipation of desirable improvements in everyday life and an anxiety that revolves around unintentional or unforeseeable negative consequences (Simon, 2004). Numerous examples of such societal reactions exist in modern history, be it after the introduction of steam engines,

trains, electricity, telephones, automobiles, airplanes, television, nuclear bombs, computers, or the Internet (cf. Simon, 2004). Many famous novels and fictional stories owe their success to their effective play on such technophobic fears. In Mary Shelley's Frankenstein, a classic within this body of literature, the fictional scientist Dr. Victor Frankenstein uses electricity to revive a monster he composed of dead body parts. Despite his good intentions, his ignorance exceeds his knowledge and he ultimately pays for his attempt to play God with his life (Shelley, 1995). The tale of Dr. Frankenstein exemplifies more than just the fears technological transgressions of unseen boundaries oftentimes evoke. It also hints at the religious dimension of technophobic fears. Several classic tales, such as the Greek tale of Prometheus, indicate that the misgiving that mankind as the creator of fundamental accomplishments interferes with the prerogatives of the gods and ultimately must pay the price for this sacrilege exists since ancient times. Throughout the long history of this fear, its prominence appears to be highly correlated to the significance of technological inventions (Edgerton, 1995). The multitude of tremendous inventions during the last century and the fundamental societal changes they have wrought have turned the peoples' fears of mad scientists, who unintentionally unleash their destructive and monstrous technological creations on us, into a dominant theme in contemporary culture (Tourney, 1992; Tudor, 1989).

Since their invention in the mid-20th century, computers, in particular, have changed almost all aspects of society and human life in unprecedented ways (Negroponte, 1996). This tremendous societal influence has turned them into today's primary projection screen for technophobic fears and anxieties surrounding technological innovations. Exacerbating societal fears of computers is the rapidity of their continuously

advancing technology. The exponential growth of computerized calculating capacities (Kurzweil, 2005) is daunting to many people who are afraid that mankind, as creation's crowning glory, will eventually be challenged by a superior artificial intelligence. The contemporary prominence of fears that mankind will be rivaled by new forms of computerized artificial intelligence is visibly reflected in the popularity of this recurring theme in popular fiction. In Stanley Kubrick's masterpiece 2001: A Space Odyssey (1969), for example, the initially philanthropic spaceship computer HAL 9000 begins killing the crew members when faced with the prospect of disconnection. The artificial intelligence system Proteus IV in Donald Cammell's Demon Seed (1977) even rapes its creator's wife in an attempt to conceive a human-machine hybrid successor who is no longer subjected to any of its boundaries (Kozlovic, 2003). Since Demon Seed, attempts of artificial computer intelligence to subdue and enslave mankind have been a recurring theme in numerous blockbuster movies, such as the Terminator and its accompanying sequels and The Matrix trilogy (Dinello, 2005).

Against this background, many hacker movies and stories can be characterized by their distinctive play on the fear of unleashed and uncontrollable technological catastrophes. In the classic hacker movie War Games (Badham, 1983), a young hacker exploits a back door into a central military computer. Not realizing that he is actually logged into a computer system that has control over the United States' nuclear arsenal, he starts playing a game of global thermonuclear war and unknowingly brings the world to the brink of nuclear annihilation. Such blurring of the line between simulation and reality is a common theme in hacker movies. In many such films, the fate of real persons, organizations, countries, or even the world is decided by actions that take place in a

contested virtual space. In eXistenZ (Cronenberg, 1999), the line between video game and reality becomes blurred in a shocking and gruesome way when a video game designer creates an artificial reality game that is played directly in peoples' minds. Similarly, the data trafficker Johnny Mnemonic (Longo, 1995) stores sensitive information directly in a cybernetic storage system within his brain and is forced to hack his own brain when parts of the secret message become lost. Already in the classic movie Tron (Lisberger, 1982), a hacker is transported into the digital universe inside a computer, where he must survive combat as a cyber-gladiator in order to stop the artificial intelligence that has taken over his computer company. The implicit suggestion of these and many other fictional and non-fictional hacker stories is that the preoccupancy of hackers with computer technology and cyberspace dehumanizes them.

Such dehumanizing depictions further reinforce the common stereotype of hackers as antisocial, reclusive, introverted, and dysfunctional hermits, whose computer-centered escapism from the social worlds of interpersonal interaction eventually endows them with superior technological skills. Similar stereotypical portraits of hackers characterize them as young male misfits and fledgling teenagers who, rather than being intimidated by the latest computer technology, embrace this technology instead. They are seen as "geeks," juvenile technophiles to whom computer technology provides an opportunity for self-realization in an environment that is not laden with the complexity and unpredictability of human interactions. By excelling in their mastery of this technology, hackers supposedly compensate for their alleged social shortcomings. Along these lines, the negative stereotype of hackers displays them as teenagers who are initially driven to their computers by social deficits and who, through their preoccupation with

computer technology, become even further detached from reality. In some instances, hackers are even seen as juveniles who are being driven by feelings of contempt and disdain toward a social environment that excludes them and who use their hacking skills as a resource for taking revenge against the persons or institutions they scorn. As one commentator notes, “the fact that hackers are also invariably young in popular perceptions is also not a coincidence – the apparent ease with which a ‘younger generation’ is able to engage with the realm of computer technology, a technology that many older people continue to see as mysteriously daunting, merely serves to sharpen the sense that all manner of extravagant things may be possible for those with the know-how” (Yar, 2006, p. 25). Thus, the portrayal of hackers as exclusively young seemingly mirrors technophobic fears that are particularly prevalent among older generations. Many members of older generations feel disconnected, left behind, and disadvantaged by the spreading of a technology that provides younger generations with the advantage of instantly accessible and virtually limitless information (Dowland, Furnell, Illingworth, & Reynolds, 1999; Negroponte, 1996). Hackers, in particular, stand out due to their mastery in manipulating and utilizing this seemingly incomprehensible computer technology, an ability that in the perception of many borders on wizardry. It is this uncertainty and weariness about the ominous capabilities of hackers that provokes technophobic fears and paints the hacker image negative.

Notwithstanding the many unfavorable components of commonly held beliefs about hackers, their public representations are not unanimously negative, but can best be described as intrinsically ambivalent. Just as technological inventions cause anxiety and fascination in equal measures, persons who master these inventions also evoke a

particular fascination and admiration. This admiration is also reflected in many movie portrayals of hackers, in which they are displayed as socially maladjusted yet brilliant heroes who use their extraordinary computer expertise to save the world from evil viruses, rampaging corporations, nuclear Armageddon, or even invading aliens. Contrasted with classic action heroes, they are no longer muscular one-man armies, but technologically sophisticated protagonists, "keyboard cowboys" (Softley, 1995), who solve the world's problems with keystrokes rather than guns.

Even though many fictional hacker characters might have had some trouble with the law in the past, they are typically displayed as essentially good-natured characters with whom viewers can identify. As Thomas (2002) points out, the criminality of hackers is oftentimes contextualized, negotiated, and relativized by the narratives themselves. In many storylines, their illegal actions are justified as being forced by others, accidents, or—most commonly—unavoidable means to expose horrible secrets, injustices, or to fight a greater evil. Thus, while seen as principally threatening because of their self-immersion into abstract, virtual, and dehumanized worlds, they are also portrayed as "freedom fighters of the 21st century" (Kovacich, 1999), heroes who either reclaim human authority over rivaling technological entities (Taylor, 2000) or fight against unjust domination by corrupt governments and megalomaniac corporations. Particularly the latter is a dominant theme in many fictional hacker stories. In Hackers (Softley, 1995), for example, a clique of juvenile hackers accidently discovers and prevents a large-scale corporate conspiracy that would have otherwise led to an ecological disaster. Similarly, a computer hacker becomes suspicious of his corrupt employer, a multinational computer company CEO that is loosely based on Bill Gates, in the movie AntiTrust

(Howitt, 2001). His investigation into company procedures confirms his suspicion and he eventually unveils a ruthless and murderous plot to dispatch the company's anti-trust problems.

Summarizing, fictional accounts and portrayals of hackers can be characterized as being inherently ambivalent in their reflection of technophobic fears and technophilic fascinations. This cultural ambivalence is not only mirrored in the positive and negative associations evoked by the terms "hacker" and "hacking," but also in surveys that examine public opinions about hackers (Dowland et al., 1999; Voiskounsky, Babeva, & Smyslova, 2000). Dowland et al. (1999) found principally ambivalent attitudes toward hackers. The study also demonstrated that the division between rather positive and rather negative opinions runs alongside generational lines. Whereas members of older generations expressed primarily anxious and negative attitudes, younger respondents tended to see hackers in an overall positive light (Dowland et al., 1999). One year later, Voiskounsky and his colleagues again found the same patterns expressed in a study conducted in Russia. In Voiskounsky's survey, young Russians expressed a particular admiration for the intriguing cleverness and intelligence they ascribed to hackers (Voiskounsky et al., 2000, p. 72-3).

Thus, the ambivalence between fears and admirations in the perception of hackers as "a schizophrenic blend of dangerous criminal and geeky Robin Hood" (Taylor, 2000, p. xii) appears to be a universal pattern in mainstream culture as well as public opinions. Yet, this ambivalence is not the only one in the common perception of hackers. While both fears and admirations are sparked by the ingenious computer skills typically ascribed to hackers, such skills are commonly seen as having been developed as

means for compensating social isolation and underdeveloped social skills. The admiration for hackers is undoubtedly caused by the inability of most people to comprehend the techniques hackers employ to manipulate computers. The explanation of such superior computer skills as a compensation for deficient social skills, however, presents an unvalidated and questionable assumption in the representation of hackers and should be scrutinized.

Both the various contested meanings of the terms “hacker” and “hacking” and the perceptions of hackers in the general public are important elements that have to be considered in a scientific study of hackers. The disputed nature of the two terms implies that researchers have to be explicit when informing study subjects about what exactly they mean by hacking. The common perception of hackers, on the other hand, has to be considered because it likely exerts an influence on the self-perception of hackers. More importantly, it is also the broader background against which a scientific understanding of hackers has to be established.

Both considerations about the meaning of hacking and hackers, while presenting contextual aspects that are necessary for an accurate understanding of hackers, are only two elements of a more complex operationalization process. Hacking as a form of cybercriminal activity is carried out in a unique environment—cyberspace. This environment exhibits several criminogenically relevant features that render it distinctively different from any other environment and need to be addressed in cybercrime studies. Thus, the next section outlines the development of the societal threat posed by cybercrimes and the distinct challenges the cyberspace environment holds for cybercrime researchers.

CHAPTER THREE:
THE GROWING THREAT OF CYBERCRIME

Riyadh, November 28, 2005. During a conference on information security in the banking sector, Valerie McNiven, a former e-finance and e-security specialist for the World Bank and current U.S. Treasury advisor on cybercrime, estimated that in 2004, financial harm from global cybercrime eclipsed the revenue generated from drug trafficking in the U.S. for the first time. According to her estimates, the revenue gained from illegal cybercrime activities was over $105 billion.

Even though from a scientific standpoint, McNiven's statement that global cybercrimes are becoming more profitable than drug trafficking, which is currently the highest-grossing illicit activity in the U.S., simply cannot be substantiated, it nevertheless hints at substantial developments in the evolution of cyber-criminality. The statement cannot be sustained because McNiven, aside from including illicit activities such as corporate espionage, child pornography, stock manipulation, phishing fraud, and copyright offenses in her estimate of total losses, also failed to recognize cross-national differences in the legal definition of what constitutes a cybercrime. Moreover, consider the fact that the estimates for many of the activities included in McNiven's definition are provided by interest groups who gladly inflate statistics to the limits of credibility. For example, the recording industry, whose estimated losses comprise a large portion of McNiven's $105 billion estimate, equates every illegally obtained copy with a direct loss of unsold merchandise, a calculation whose inflation is inherently obvious (Leyshon, Webb, French, Thrift, & Crewe, 2005; Marshall, 2004). Gauging the financial harm of

the crimes included in McNiven's cybercrime definition is fraught with problems, and the empirical evidence upon which McNiven's claim is based is clearly preliminary, thus rendering its validity questionable.

In spite of the methodological flaws of the estimate, McNiven's statement is nevertheless important because it points to significant developments in the area of cybercrimes. FBI statistics from recent years suggest that the financial damage caused by cybercrimes increases between 20% to 35% each year (L. A. Gordon et al., 2005; L. A. Gordon, Loeb, Lucyshyn, & Richardson, 2006), thereby likely surpassing the drug trade in terms of growth rate. The prolific growth of the Internet in terms of the number of users, functionality, and efficiency of electronic business procedures has convinced many industries to move their operations, and most importantly their money, online. Online shopping, online banking, online stock broking, credit card gateways for wire transfers, and e-commerce all provide opportunities to make business processes more efficient. On the other hand, the use of the Internet for the transfer of financial resources has drawn many criminals to this new medium (Newman & Clarke, 2003). The temptation toward the profit that can now be gained online has completely changed the face of cybercrime (Schell et al., 2002). In order to provide a better understanding of cybercrime phenomena as they exist today, the following section provides a brief summary of the co-evolution of the Internet and cybercrimes.

The Co-Evolution of the Internet and Cybercrimes

Misuse of computer systems is not a new phenomenon. In fact, the abuse of computer systems is as old as the technology itself, but cybercrime was a phenomenon

of no significance before computer networks were developed. The reason is a practical one: When information is stored locally without being networked, it is much more difficult to gain access to than it is to intercept information that is transferred across physical distances within a network. Another advantage is that access to one element in the network can possibly provide access to other vulnerable computers in the same network. However, even in the early days of computer networks, cybercrime was still in its infancy and of little societal significance. In these times, computers were rare, very expensive, and required specialized knowledge to be operated successfully. All these factors inhibited widespread use and misuse.

The importance of the Internet, and with it, the significance of cybercrime began to slowly grow as computing became easier and less expensive. In the 1970s, the first affordable personal computers appeared and ARPAnet, the predecessor of our current TCP/IP based Internet, was created (Hafner & Lyon, 1998, p. 40-41). Nevertheless, even as Internet use became more widespread, connecting computers to it was quite a difficult undertaking. Existing operating systems provided no software to connect to Internet Service Providers, which at the time were few and very expensive. Access to the Internet was a privilege reserved for a few researchers, military personnel, government agencies, and technology experts who used it primarily to exchange highly specialized information (Vallee, 2003). Computer crime first drew the attention of legislators after ISPs such as AOL, CompuServe, and Prodigy began to provide software that made it much easier to connect to their services (Naughton, 2000). In 1986, alarmed by the rising number of cyber-trespasses, the U.S. government passed the Computer Fraud and Abuse Act (U.S.C., 1986), the first legislative act that made breaking into computer net-

works illegal. It is worth mentioning that this first legislative effort did not apply to juveniles, a circumstance that is inconceivable today. Hackers at the time were skilled computer experts motivated primarily by curiosity to explore other systems' weaknesses, to reveal their configurations and operations, and to take advantage of the technical possibilities of networked computing (Graham, 2004). Many of them followed an ethical code that disallowed them to inflict damage on the hacked system. Early hackers who followed this code distinguished themselves from so-called "crackers," hackers motivated by malevolent intentions aimed at exploiting the hacked system (Schell & Martin, 2004).

In the 1990s, Internet prices dropped dramatically and the Internet began to grow exponentially. Today, computers are omnipresent in our daily lives. A modern society without computers or the Internet has become unthinkable. The Internet has developed into an essential, mission-critical infrastructure for government agencies and organizations, almost all private business industries, and financial institutions (Li, 2006). Among many other aspects, manufacturing routines and processes, water supplies, electric power grids, air traffic, and stock markets are essentially operated, managed, and controlled through computer networks (Painter, 2004). E-commerce is growing with yearly increase rates of 20%, reaching a total volume of $116 billion today (Richtel & Tedeschi, 2007). Today, 44 million citizens in the U.S. have online bank accounts and the online banking population in the U.S. grew by 9.5% in 2006 (Warner, 2007). Also, a third of the U.S. workforce is online, an important factor since more than half of all e-commerce transactions are work-related (Alaganandam, Mittal, Singh, & Fleizach, 2005). The financial value of Internet activities and the wealth stored on computer systems has reached unprecedented dimensions and attracts criminals that are no longer motivated

by technical curiosity, but rather by financial motives. Today's societal dependence on the Internet, and particularly the use of the Internet for banking and commercial transactions, has fundamentally changed the face of cybercrime. The early hacker population of highly skilled computer experts motivated primarily by technical curiosity has given way to a wide array of criminals with varied skills, knowledge, resources, authority, and motives. Profiles of today's offenders range from teenagers to disenchanted employees, traditional criminals, organized racketeers, or even foreign intelligence agents. The present-day dimensions of the term 'cybercrime' encompasses a vast scale of multi-faceted phenomena ranging from small-time pranksters to organized crime circles as well as nationally funded spies (Bednarz, 2004).

The many dimensions and different methods of today's cybercrimes and the multitude of offender profiles, in combination with modern society's dependency on computer technology, necessitates an accurate assessment of the risks and threats in order to answer the question of how to combat computer criminals effectively. Protection against the various methods of cyber-criminals and the ability to trace, capture, and prosecute them require research in order to provide an accurate assessment of the current landscape of cybercrimes and the threat they pose. Empirical research is vital for the design of effective countermeasures to combat not only hackers, but also other newly emerging types of cyber-criminals. Only then is it possible to minimize the potential for harm in the online environment. The salience of cybercrime stems from its increasing societal relevance, and mainstream criminology is slowly starting to grasp the extent of the problem.

The Novelty of Cyber-Criminology

Researchers have observed the emergence of cyberspace as a new realm for criminal activity since the 1990s (Littlewood, 2003; Thomas & Loader, 2000; Yar, 2005b), yet mainstream criminology has long been negligent towards the problem of cybercrime and has failed to recognize its societal relevance (Jaishankar, 2007; Jewkes, 2006; Mann & Sutton, 1998). The study of cybercrime has only recently gained widespread attention among criminologists. Several indicators demonstrate that the study of cybercrimes is only now catching up with the developments and methods of cyber-criminals. The first conference devoted entirely to cybercrime, the "Cyber Criminology and Digital Forensics Initiative Conference", took place in Spokane Valley, WA, USA in October 2006 (Jaishankar, 2007). Probably the strongest indicator of the recent establishment of cyber-criminology as a distinct subsection within criminology is that the first interdisciplinary research journal dealing exclusively with cybercrime, the International Journal of Cyber Criminology (IJCC), was first published in January 2007 (Jaishankar, 2007). Another indicator that the field is just now gaining popularity is the growing number of scholarly publications addressing the various aspects of cybercrime (Furnell, 2002; Yar, 2006). Empirical publications require data to analyze and explain cybercrime phenomena. The small number of publications is partly attributable to the small number of surveys and datasets available to researchers. For example, the first nationally representative survey, the National Computer Security Survey (NCSS), which was sponsored by the U.S. Department of Justice (DOJ), Bureau of Justice Statistics

(BJS), and the U.S. Department of Homeland Security National Cyber Security Division (NCSD), was fielded in 2006.

Taken together, these indicators suggest that criminological studies of cyber-crime are in their early stages and that more attention must be devoted to this pressing new form of crime. In other words, “A new, radical discipline named cyber- criminology is the need of the hour to explain and analyze the crimes in the Internet” (Jaishankar, 2007, p. 1). In addition to the relative lack of publications and empirical data, this new discipline faces a range of problems and difficulties. Some researchers even question whether cybercrime is a qualitatively new form of crime justifying the establishment of a distinct subsection within criminology. Thus, the headmost question is whether cyber-crimes constitute a unique type of crime.

The Novelty of Cybercrime

Some researchers argue that from a legal standpoint, cybercrimes are largely the same as ‘old-fashioned’ non-virtual crimes committed with new tools and nothing else than the “same old wine in new bottles” (Grabosky, 2001, p. 243). However, there is broad consensus among the majority of researchers within this newly-developing sub-section of criminology that society is confronted with a new type of crime that has distinctly different qualities from ‘terrestrial’ crimes. Most cybercrime researchers, particularly criminologists with a sociological background who examine the social-structural conditions of the environment in which the crimes are committed, insist that it presents a radically new and distinguishable form of crime. Social interactions, in large part, are

determined by the possibilities imposed upon or restricted by the structures of the environment they are taking place in.

Cyberspace, a term coined by William Gibson in his famous science-fiction novel Neuromancer (1984) and later defined as “there’s no there, there” (Gibson, 1988, p. 40), presents an electronic universe of information resources available through computer networks. Social interactions taking place within this world of connected computers are markedly different than in the ‘meatspace’ (Pease, 2001, p. 23). The Internet, as the largest of these electronic information networks, “variously ‘transcends’, ‘explodes’, ‘compresses’, or ‘collapses’ the constraints of space and time that limit interactions in the ‘real world’” (Yar, 2006, p. 11). It represents the most important element for the ‘time-space compression’ of globalization (Harvey, 1989), in that it allows nearly instantaneous interactions between spatially distant actors.

Furthermore, the Internet offers various degrees of automatization in interaction, thereby creating ever-new forms and possibilities of social exchange (Shields, 1996). Among various other aspects, automatized interactions within computer-mediated communication (CMC) networks extend both the scope and scale of offending, as the aforementioned examples of the Turkish hacker and the attacks on Estonia’s digital infrastructure demonstrate. Many-to-many communications inexorably alter the relationships between offenders and victims, as well as the possibilities of criminal justice systems to counteract or resolve such crimes (Capeller, 2001). Internet users are instantaneously targetable by the largest known pool of potential offenders from all over the world. Hackers are not bound by the limits of physical proximity and can strike by launching highly automated attack routines. A wide variety of specialized software ap-

plications such as network crawlers, sniffers, and scanners exist that can be used to execute such attack routines. These programs perform automatic scans of wide ranges of IP addresses for vulnerabilities. CMC allows individual users to reach, interact, and affect thousands of other users simultaneously. Thus, the possibility for potential offenders to target large quantities of other users and their property is multiplied to an unprecedented degree. Electronic communication networks are unique 'force multipliers' that can be abused to create enormous negative effects with only very limited resources and efforts. One example of the misuse of the Internet as a force multiplier is the distribution of viruses, worms, trojan horses, root kits, and other malicious code; another is the daily flood of mass-distributed 'spam' emails. The research institute IDC estimates that in 2007, 40 billion of the nearly 97 billion emails sent daily will be spam messages (Levitt, 2007). According to their report, the worldwide volume of spam email sent is expected to exceed the volume of person-to-person emails sent for the first time in 2007.

Another criminogenically relevant feature of CMC networks is that they allow for easy creation, alteration, and reinvention of the social identity. Internet users can create arbitrary virtual avatars, electronic representations and identities that are not required to be analogous to their 'real world' identities (Turkle, 1995). The ability to disguise social identity is of high criminological relevance because it allows potential offenders to remain anonymous (Snyder, 2001). The increased anonymity in electronic communication networks lowers the offender's perception of the risks involved in the commission of cybercrimes. As with terrestrial crimes, anonymity in cyberspace ultimately raises the likelihood that a cybercrime is committed (Joseph, 2003).

From the above, it can be concluded that three features of these electronic networks create new forms, patterns, and structures of illegal behavior: the irrelevance of tempo-spatial distances, the unlimited potentiality of many-to-many connectivity, and the possibility to disguise oneself behind arbitrary, anonymity-granting identities. These features of the cyberspace environment render all interaction taking place within it, including cybercrimes, original and distinctly different from interactions in any other social environment known before.

The above characteristics of digital crimes justify the establishment of cybercriminology as a distinct subsection within criminology. They also pose new challenges for both researchers and law enforcement alike which require innovative responses. The challenges for the criminal justice system arise in particular from the global dimensions and the borderless nature of the environment. Disparate criminal laws and geographical boundaries of jurisdictions pose important limitations for law enforcement efforts because they have no direct equivalent in cyberspace (Koops & Brenner, 2006). Many hackers take advantage of this fact by deliberately exploiting sovereignty limits and cross-jurisdictional differences. Though internationally cooperative efforts to harmonize Internet laws, such as the groundbreaking Council of Europe's Convention on Cyber Crime, are being undertaken, large gaps remain in the realm of international cybercrime legislation.

In addition to the legal complexities resulting from the global nature of the problem, there are challenging technical intricacies. These complications include the volatility and intangibility of evidence owing to the lack of traditional forensic artifacts such as fingerprints, DNA, or eye-witness accounts associated with these types of offenses

(Shinder & Tittel, 2002). Hackers enjoy a high level of anonymity stemming from anonymizing services, encryption algorithms, 'spoofing' tools, and the increasingly widespread availability of Internet cafés and public wireless networks (Computer Crime and Intellectual Property Section, 2002). To make matters worse, legislative efforts to force ISPs to keep log files documenting user data long enough to conduct criminal investigations have not yet been successful. Each of these technical obstacles and time constraints raises the cost of cybercrime investigations far above the cost of traditional crime investigations. Presently, law enforcement does not have the required resources and experts with specialized technical knowledge necessary to track and apprehend a large portion of online offenders. One indication for this lack of resources is the estimate that the chance for being prosecuted for hacking in the US is one in 10,000 (Bequai, 1999). Hence, even in jurisdictions with appropriate laws to counteract digital crimes, the implementation of sanctions remains restricted by logistical and financial limitations.

The preceding discussion delineated the problems that the new features of cybercrimes pose for law enforcement. Central to this study, however, are the unique challenges that arise in cybercrime research. The qualitatively new features complicate the research endeavor in several ways. These complications are addressed in the following chapter.

CHAPTER FOUR:
THE CHALLENGES IN RESEARCHING CYBERCRIME

The valuable information gatherable only through criminological research on cybercrimes is required for addressing and counteracting this growing societal threat, but the developing field of cyber-criminology has yet to overcome a series of distinct methodological and theoretical problems other research areas have already mastered. The foremost methodological problem is that, currently, no universally agreed on criminological definition of the term cybercrime exists. This problem is fundamental because of its implications for the operationalization of the concept and is, therefore, discussed at the beginning of the current chapter.

Methodological Problems

The Problem of Defining and Classifying Cybercrimes

The investigation of cybercrimes is a relatively new field in criminology and, as such, it is confronted with several methodological problems that other areas have already overcome. One main problem in the operationalization of the concept is the absence of an widely agreed on criminological definition of what constitutes a cybercrime. The problem is further exacerbated by the fact that the complex concept cybercrime encompasses multiple dimensions and various manifestations. The term cybercrime denotes a wide range of phenomena ranging from an attack against essential national infrastructure systems, such as the National Grid, to fraudulent manipulations of penny

stocks in chat rooms and bulletin boards. This vast variety of phenomena subsumed under the term makes it difficult to provide a precise definition in terms of aggregate incidence and impact. Wall also reminds us that even though the term cybercrime has considerable currency in discourses within the media, politics, academics, and the public, it still has “no specific referent in law” (Wall, 2001, p. 2). The term is often understood as signifying an array of illegal acts whose commonality is that they are conducted through electronic information and communication networks. An example of such a general definition is the one proposed by Thomas and Loader, who summarize all “computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks” (Thomas & Loader, 2000, p. 3) under the term cybercrime. Under this definition, the novelty of cybercrime is that it is conducted in the ‘virtual space’ of worldwide networks of information exchange through interconnected computers, particularly the Internet (Castells, 2002). The term ‘conducted’, in this context, can refer to computers and networks functioning as the agent, facilitator, or the target of criminal activity.

Within this broad conception of cybercrime, certain types of activities included in the term are commonly distinguished. Typically, types of cybercrimes are categorized by the function technology has in their commission. Furnell differentiates between ‘computer-assisted crimes’, such as fraud, theft, sexual harassment or pornography, in which “the computer is used in a supporting capacity, but the underlying crime or offense either predates the emergence of computers or could be committed without them,” and ‘computer-focused crimes’, such as hacking, website defacing, spamming, or launching of virus/worm attacks, “cases in which the category of crime has emerged

as a direct result of computer technology and there is no direct parallel in other sectors" (Furnell, 2002, p. 22). A similar distinction is proposed by S. Gordon and Ford (2006), who isolate three main dimensions of the term cybercrime: (1) The computer and hardware device dimension, i.e. the role technology plays in the conduct; (2) the technology – human element continuum, a dimension that ranges from cybercrimes that are primarily technological in nature to those that have pronounced human elements, like for example cyber-stalking; and (3) the 'crimeware' focus, a term S. Gordon and Ford use to denote software whose primary application is the commission of cybercrimes. Unfortunately, Furnell's as well as S. Gordon and Ford's classifications, while being useful in analyzing interdependency processes in social and technological developments, are of limited criminological value.

One alternative is suggested by Wall (2001, pp. 3-7), who translates four existing criminal law classifications into their cybercrime equivalents. He distinguishes between: (1) '(cyber)-trespass', the unauthorized crossing of the boundaries of computer systems and/or the causation of damage to those systems or their possessors; (2) '(cyber)-deceptions/theft', stealing of money or property, e.g. credit card fraud, identity theft, or violations of intellectual property a.k.a. 'piracy'; (3) '(cyber)-pornography/obscenity', all pornographic, violent, hate-filled, racist, or generally offensive activities breaking obscenity and decency laws; and (4) '(cyber)-violence', the infliction of psychological harm, or the incitement of physical harm, e.g. hate speech, 'flaming', harassment, stalking, or the distribution of information assisting in dangerous activities such as bomb-building. By emphasizing the origins of cybercrimes in traditional crime categories, Wall pursues a conservative approach. Each of his four categories subsumes rather broad and di-

verse ranges of phenomena, a circumstance that calls the validity of his typology into question.

A practical solution to the challenge of defining cybercrimes is offered by Ralph D. Clifford (2006). Instead of continuing the debate with just another proposed definition, Clifford and the team of legal experts he assembled question the practicality of attempting to subsume the vast scale of multifaceted phenomena that is encompassed by the term cybercrime under one legal definition. In this regard, Clifford's approach presents an important conceptual break that calls into question the appropriateness of the very debate surrounding the legal definition of the term cybercrime. Instead of continuing the academic search for one overarching legal definition, the approach taken in this second edition is to examine the practical implications for investigators, prosecutors, and defense attorneys of the various cybercrime-related statutes (Bachmann, 2008). Despite Clifford's suggestion to end the debate about an overarching definition this debate will likely continue, and eventually, a sound criminological definition will be proposed. Until then, Clifford's approach seems to be the most practical solution because it is best fitted to address the vast variety of criminal activities subsumed under the term cybercrime.

The Problem of Measuring the Scale of Cybercrimes

Obtaining an accurate assessment of the scope and severity of cybercrimes is a difficult undertaking. Unfortunately, this is true for many of the types of offenses studied by criminologists. Official crime statistics, for instance, do not objectively measure incident trends and distributions, but are socially constructed. Official datasets include only crimes that have been reported, and there are several reasons why crime victims can

be reluctant to report offenses. These reasons range from perceptions of the offense as a private matter or as trivial to fears of retaliation, unawareness of the victimization, embarrassment due to the victimization, or lack of faith in an effective response. Especially corporate actors oftentimes also fear the potential damage the reporting of their victimization can have for their public reputation. Another major problem is that even when offenses are reported, they may be excluded from the Uniform Crime Report (UCR) because only the primary charges in each incident are recorded. Fortunately, this problem has been resolved in the National Incident Based Reporting System (NIBRS), which includes all charges in the incident report as well as several situational variables. A related under-reporting problem that remains unresolved in both national datasets arises from the circumstance that they rely on police reports which are submitted on a voluntary basis. In addition to the many obstacles challenging cross-sectional measurements, longitudinal datasets oftentimes also have to resolve issues resulting from changing legal classifications.

While the aforementioned problems are faced by all quantitative criminological studies, they are magnified with respect to hacking attacks and, to varying degrees, to all other forms of cybercrimes. As was stated previously, the intangibility of evidence and the lack of traditional forensic artifacts make online offenses more difficult to detect than terrestrial crimes. Complicating matters further is the remaining lack of knowledge of many as to what exactly constitutes a cybercrime, and consequently, whether reporting of a particular incident is appropriate (Howell, 2007). Moreover, the global nature of cybercrimes and the high level of offender anonymity in the online environment are two additional aspects that discourage both victims and law enforcement from reporting

such crimes because they decrease the perceived chance of apprehending the offender. As a result, many police stations prioritize reporting of local problems (Wall, 2001) occurring on their “patch” (Lenk, 1997, p. 129). Taken together, the above factors justify the conclusion that cybercrimes are greatly under-reported in official statistics. In 2000, Detective Sergeant Clive Blake from the Metropolitan Police Fraud Squad estimated that as few as 5% of computer crimes are actually reported (Blake, 2000).

Crime and victimization surveys offer an alternate assessment of crime levels. Victimization surveys are often used by criminologists because of their ability to encompass offenses that are typically under-reported in official statistics. Despite their advantages, crime and victimization surveys cannot completely eliminate all of the difficulties faced by official measurements. To begin with, it is self-evident that an undetected crime cannot be reported. Of higher importance for the quality of survey data, however, are systematic errors and the bias they introduce. Systematic errors can result from many different sources, such as incongruities in the definition of what constitutes a crime between interviewer and interviewee, various other interviewer effects, the presence of third persons, sponsorship-biases, or the so-called response set of the participant to name but a few. Survey researchers have long recognized that even the highest possible optimization of survey instruments will never completely eliminate survey errors (cf. Groves et al., 2004). Despite their shortcomings, victimization surveys are especially relevant for cybercrime studies because official data on computer offenses remains scarce. Unfortunately, survey-related problems are again exacerbated when measuring cybercrimes. Cybercrime victimization surveys typically have decidedly selective populations and study samples. The majority of surveys, including the annual CSI/FBI Com-

puter Crime and Security Survey, measure only corporate or organizational victimization and exclude private computer users. Wall (2001) also hints at the various existing inter-survey inconsistencies with regard to methodologies and classifications. These inconsistencies complicate meaningful comparative analyses and aggregations. Yar lists three more reasons for under-reporting by corporations and organizations that are subject to public scrutiny. He states that public actors “may prefer not to acknowledge victimization because of (1) fear of embarrassment: (2) loss of public or customer confidence (as in the case of breaches relating to supposedly secure e-shopping and e-banking facilities): and (3) because of potential legal liabilities” relating to their violation of data protection responsibilities (Yar, 2006, p. 14).

All the above mentioned difficulties suggest that more studies and improved measurement techniques are needed, and they should lead cybercrime researchers to be cautious about the validity of their data. However, they do not imply that researchers should refrain from using all available data. To the contrary, more current data are needed for a greater understanding of the limitations and for the refining of methodological techniques to better address them.

Eventually, meta-studies of official data and victimization surveys will be able to provide a reasonably adequate picture of the threats Internet connected computer users are facing. When pursuing this approach, however, one has to be cautious in drawing conclusions about the offenders because the high degree of anonymity and inaccessibility granted by the Internet environment conceals many relevant offender characteristics to the victims, and the low apprehension rate prevents accurate estimates of systematic differences between offenders who get caught and those who do not. In addition

to these measurement issues, cyber-criminologists face certain theoretical problems that are addressed in the following section.

Theoretical Problems

Attempts of criminology to uncover the underlying causes of criminal behavior in cyberspace are inevitably based on data and theories relating to terrestrial crimes. Differences in the cyberspace environment with regard to structural and social features call into question the transferability of traditional criminological theories to cybercrimes. Presently, the applicability of mainstream criminological theories is yet to be determined. Two particular problems arise from questions relating to who commits cybercrimes and where are they committed.

The Problem of Isolating Structural Correlates

The first problem arises from the circumstance that many criminological theories, in varying degrees, rely on ecological and environmental propositions. These theories explain crimes as phenomena that occur within particular settings exhibiting specific social, cultural, and economic characteristics. For example, routine activities theories focus on the time-space convergence of motivated offenders with suitable targets and the absence of capable guardians, thereby implying certain environmental settings in which offenses can occur (Cohen & Felson, 1979; Felson, 2000).

Disorganization and other theories that focus on ecological factors have initiated crime mapping projects as well as several measurement and prevention programs aimed at the removal of criminogenic factors from the environment (Akers & Sellers,

2004). Nonetheless, such approaches are problematic when transposed to the context of cybercrimes. The virtual cyberspace environment within which cybercrimes are committed has no equivalent to easily distinguishable terrestrial locations. Rather, cyberspace has to be understood as “fundamentally and profoundly anti-spatial” (Mitchell, 1995, p. 8), an environment in which there is no physical distance between locations. The irrelevance of spatial distances within cyberspace renders all criminological theories relying on assumptions specific to terrestrial environments handicapped for the explanation of cybercrimes.

The Problem of Isolating Offender Characteristics

A different group of criminological theories examines the reasons why some individuals repeatedly involve themselves in criminal activity while others abstain. These theories correlate specific categories of crimes with certain social characteristics of the offender. An example of these corresponding characteristics can be illustrated using property crimes and violent crimes. Such offenses are primarily committed by persons at the lower end of the income distribution. Other social characteristics predisposing individuals to commit property or violent crimes might include lack of educational attainment or involvement in deviant subcultures. There is a significant amount of empirical evidence within the criminological literature substantiating this correlation between economic disadvantage and engagement in these types of crimes. The same correlation, however, cannot be established in the case of cybercrimes.

To the contrary, the aforementioned correlation is reversed with regard to computing skills and Internet access, in that the more disadvantaged segments of the econom-

ic and educational distribution possess them the least (Yar, 2006). At the same time, individuals with the economic and intellectual resources necessary for the commission of cybercrimes usually come from more socially advantaged backgrounds. Internet offenders typically exhibit characteristics that are substantially different from the attributes of the majority of other criminals (Wall, 2001).

The two theoretical problems associated with the identification of ecological and individual characteristics of cyber-offenders render many traditional criminological theories that focus on environmental and individual factors unable to explain of Internet crimes. This circumstance has led some cyber-criminologists to suggest that the appearance of cybercrimes and the inability to simply transpose traditional empirical assumptions and explanatory concepts to them may require considerable theoretical innovation. Criminology may need to develop new analytical tools to adequately assess these qualitatively new crimes (Yar, 2006).

Recognizing these new conceptual challenges, Ronald Clarke suggested a rather radical solution. His memorable and highly controversial suggestion is to completely suspend criminological inquiries into the motivations of cyber-offenders, and instead focus solely on the crime reduction strategies provided by the 'crime science' approach (Clarke, 2004). Diverting from the attempts of criminology to unveil causational crime factors, crime science merely attempts to reduce it through suitable prevention and detection solutions. Crime science utilizes computer science, engineering, and the physical sciences as much as the social sciences, and resorts to the fields of statistics, environmental design, psychology, forensics, policing, economics and geography to exclusively study the characteristics of crime incidents, while ignoring the traits and motiva-

tions of criminal actors. Crime scientists substitute the analytical tools of traditional criminology such as cohort studies, criminal career studies, and regression analyses with methods that include crime patterning, hot spot analyses, and crime mapping studies. Clarke demands that criminologists focus on concrete and manipulable factors of crime events and accept the remainder as immutable facts. This suggestion is in line with his prior work in the area of situational crime prevention and rational choice approaches (Clarke, 1992; Clarke & Cornish, 1985, 2001; Clarke & Felson, 1993; Cornish, 1994; Cornish & Clarke, 1986), because these theories consider criminal behavior to be indifferent from any other behavior place, and their central focus is on the reduction of opportunities inducing criminal activities.

The Proposed Theoretical Approach

The approach taken in this research project is based on the argument that first, crime science and the attempts of traditional criminological theories to explain crime causation are not mutually exclusive. To the contrary, they can be reciprocally beneficial. Crime science models striving to reduce crime are necessarily based on at least implicit assumptions of causational factors and characteristics of criminals. Thus, the knowledge and insights gathered through traditional criminological theories can increase the validity of crime science models and make them more accurate. Crime science models, on the other hand, have the potential to reveal insights that allow inferences and conclusions about crime causation factors, and can thereby contribute to advancing criminological theories.

Second, it is argued here that, given the current absence of a criminological theory specifically designed to meet the characteristics of the online environment and the challenges arising from them, modeling decision-making processes which lead to the commission of criminal acts seems to be a promising approach. Such models are developed mainly in the context of rational choice approaches which attempt to reconstruct decision making processes of criminals in order to isolate manipulable factors with the potential to reduce crime. A few examples already exist in the criminological literature that demonstrate how rational choice and situational crime prevention models can be successfully applied to the area of cybercrimes (D'Arcy, 2007; Newman & Clarke, 2003).

For a number of reasons, rational choice and situational crime prevention models appear to be well suited to the application of cybercrimes. Unlike many other criminological theories, they do not rely on the particular assumptions of disadvantaged social environments or individuals, and thus are not affected by the associated problems mentioned earlier. The only assumption they make about the offending persons is that they deliberately choose to commit the criminal act because they consider it beneficial. The sole proposition of rational choice models with regard to human actors is that they use their cognitive resources to weigh the potential benefits of an action against its potential costs, and that this calculation can be manipulated through changes in the parameters of estimated risks and costs.

In the case of cyber-criminals, it is reasonable to assume that offenders premeditate their actions before they decide to commit a criminal act. All different types of cybercrimes require detailed planning in different stages of their commission and have to

be committed in a decidedly rational and deliberate manner in order to be successful. Carrying out cyber-trespasses, cyber-thefts, deceptions, or frauds, requires the offender to carefully consider and weigh alternative routes of action, select the techniques and tools appropriate for the attack, and identify exploitable weaknesses, to list but a few decisions. As was delineated in the first chapter, cyberspace exhibits several features that can lead a rationally-acting person to the conclusion that committing crimes in this environment is a viable option. Among them are the reduced risk of being apprehended, the multitude and instant accessibility of suitable, unprotected targets, and the high degree of anonymity. Clearly, crimes in the digital worlds of information exchange are the result of reasoning processes of rational calculation, purposive self-interest, and low-cost opportunities. All these aspects suggest that the engagement in cybercrime activities can appropriately be modeled as a series of decision-making processes, and that rational choice and situational crime prevention models are particularly well suited for application to cybercrimes.

CHAPTER FIVE:
THE RATIONAL CHOICE PERSPECTIVE

As a theoretical concept, rational choice revolves around the notion that crime is chosen because it appears as a promising and rewarding alternative to the offender. Although contemporary versions of this theory have appeared only relatively recently when compared to other mainstream criminological theories, the depiction of choices in terms of benefits and costs has a long tradition in economic as well as sociological and criminological thought. Within criminology, the description of offenders as rational decision makers weighing their alternatives for their pursuit of self-interest dates back to classical writers of the 18th century, such as Beccaria (1764) and Bentham (1789). Today, several different versions of rational choice theory exist, and rational choice theory has become one of the main theoretical concepts that is addressed in nearly every criminological textbook (Hechter & Kanazawa, 1997).

The criminological rational choice model that has attracted by far the most scientific attention, the so-called rational choice perspective, was developed by Cornish and Clarke in the 1980s (Clarke & Cornish, 1985). Since the theoretical underpinnings of this dissertation follow the rational choice perspective as outlined by Cornish and Clarke, a detailed description of this perspective is provided in the following section.

The Six Basic Propositions of the Rational Choice Perspective

Essentially, Cornish and Clarke's rational choice perspective model rests on six basic propositions, which are stated as below (Clarke & Cornish, 2001, p. 24):

1. Crimes are purposive and deliberate acts, committed with the intention of benefitting the offender.
2. In seeking to benefit themselves, offenders do not always succeed in making the best decisions because of the risks and uncertainty involved.
3. Offender decision making varies considerably with the nature of the crime.
4. Decisions about becoming involved in particular kinds of crime (involvement decisions) are quite different from those relating to the commission of a specific criminal act (event decisions).
5. Involvement decisions can be divided into three stages – becoming involved for the first time (initiation), continued involvement (habituation), and ceasing to offend (desistance) – that must be separately studied because they are influenced by quite different sets of variables.
6. Event decisions include a sequence of choices made at each stage of the criminal act (e.g., preparation, target selection, commission of the act, escape, and aftermath).

These six elements comprise the core of the rational choice perspective. Cornish and Clarke claim that the combination of these propositions provides a framework applicable to all different types of crimes and therefore of the largest possible criminological scope (Clarke & Cornish, 2001). The wide scope of applicability is due in part to the

concise, yet abstract and all encompassing nature of the statements, which also renders the theory decidedly parsimonious and internally logically consistent. While all six propositions are essentially hypotheses themselves, only the second one lends itself to more explicit and better testable hypotheses when applied to the context of hackers. Thus, the hypotheses of this study are derived from the second proposition. The others, on the other hand, are statements of such general and abstract nature that they cannot be operationalized in the same way. Nevertheless, propositions four to six are important guidelines for the theoretical framework structuring the assessment of hackers, their hacking careers, motivations, and various decision-making processes in the present study. The six propositions, as well as the hypotheses and the models derived from them, are addressed in greater detail in the following section.

The Rationality of Criminal Acts

The starting point of the theory essentially states that crimes are never senseless or random acts. Rather, they are seen as purposive acts intended to benefit the offender. Beneficial outcomes are most obvious in the case of money and material goods, but benefits can also include excitement, fun, prestige, sexual gratification, defiance or domination (Clarke & Cornish, 2001). This first assumption has sparked considerable criticism from numerous theoretical camps, who concede that certain crimes, particularly pathological crimes or crimes committed by mentally ill persons cannot be adequately conceptualized as rational acts. The dispute over whether all crimes are rational or not and whether the scientific reconstruction of all crimes as rational acts renders the concept of rationality universal, tautological, and thus deprived of its explanatory capa-

bilities shall only be mentioned here (Akers, 1990; De Hann & Vos, 2003). However, it is not addressed in greater detail because, for the reasons listed earlier, it is reasonable to assume that hacking attacks (as well as probably all other forms of cybercrimes) are deliberately premeditated acts that involve substantial amounts of rational considerations. Consequently, these types of criminal acts fall well within the scope of the rational choice perspective and should be at least potentially explainable with this theoretical concept.

The Limitations of Rationality in Decision Making Processes

While hacking attacks are criminal acts that do require a considerable degree of premeditation, this circumstance does not automatically imply that all hackers always make the best decisions. This second proposition is one that separates the different models and versions of rational choice theory. All rational choice models have in common that they predicate crime as resulting from choices, but they vary considerably in what they define as a rational choice. Proposing a typology of rational choice models, Opp (1997) suggests distinguishing rational choice models along a continuum ranging from wide to narrow concepts of rationality. Wide concepts of rationality, such as the one employed by the rational choice perspective, conceptualize individual decision making processes as being inevitably bounded or restricted. These models take into consideration that decision-making processes are always limited by situational and cognitive constraints. They are consistent with psychological theories depicting humans as 'cognitive misers' who strive to conserve energy and reduce cognitive load (Fiske & Taylor, 1984). They also take into account that decision-making processes include un-

certainties because they are hardly ever based on knowledge of all relevant facts and risks. Likewise, it is often impossible to gauge both the exact utility of action alternatives and the probability that this utility will indeed be the outcome of that action alternative.

Such constraints of cognitive information-processing abilities lead human actors to employ heuristics and biases in the decision-making process. For example, instead of considering every single relevant detail, offenders often rely on general tactics and methods that they have had positive experiences with in the past. Once they decide to commit the crime, they tend to reinforce their decision by focusing on the potential rewards rather than the risks. This focus on rewards rather than risks prevents offenders from accumulating the cognitive strain that would result from focusing on the dissonant cognitions of engaging in criminal activity while potentially having to suffer the consequences of punishment (Festinger, 1957). In cases where offenders take risk considerations into account, they most often focus on the short term costs of getting caught as opposed to long term consequences, such as getting punished for their actions.

'Wide' rational choice conceptualizations further acknowledge time constraints that are necessarily involved in decision-making situations. Time itself is a valuable resource, and a disproportionate time investment into considerations over low stakes decisions would not be purposively rational. Since wide rational choice models recognize cognitive and situational imperfections, they can be considered more psychologically and sociologically plausible. They assume that offenders, like the rest of us, use "satisficing rather than optimizing" (Clarke & Cornish, 2001: 25) decision-making efforts and strategies. Sometimes limitations of time, cognitive resources, and available information can lead to decisions that appear irrational.

Moreover, as Cacioppo and his colleagues have shown, individuals differ in their personal need for cognition (Cacioppo & Petty, 1982). Whereas some persons prefer analytic and rational approaches when processing information and making decisions, others tend to rely more on their faith in intuition (Cacioppo, Petty, Kao, & Rodriguez, 1986). Individuals who rely on their faith in intuition are generally greater cognitive misers than persons with a strong need for cognition. They oftentimes use heuristics, base their decisions on similar prior experiences, tend to abbreviate decision-making processes, and terminate them earlier. Rational choice theorists, however, contend that, regardless of the actual degree of rationality involved, to the offenders themselves the selected action alternative appears as the most promising one at the moment it is selected. Thus, while limited, the decision should nevertheless be considered rational.

Several testable hypotheses can be derived from this second proposition for this study. Hacking is a complex and difficult undertaking, and successful hacking requires not only extensive knowledge and expertise, but also considerable cognitive efforts. Thus, compared to hackers with a preference for more heuristic, intuition-based thinking styles, hackers who prefer to think more analytically and rationally are expected to be more successful in their hacks because they weigh more alternatives, consider more factors, and operate more cautiously. It has to be noted that, in the context of hacking, success refers to the accomplishment of gaining access to the target, and the rating of a hack as successful is ultimately a subjective assessment by the hacker. The more deliberate preparation of hackers with a preference for rational thinking styles should further result in longer preparation times for hacking attacks, and in a generally higher risk estimate, in a more risk-oriented focus. The same patterns can be expected for hackers

with a lower risk propensity because of their more careful consideration of the involved risks. Higher risk propensity, on the other hand, should lead hackers to engage in more hacking attacks because they are less concerned about the involved risks. Precisely stated, the following testable hypotheses can be formulated for the current study:

H1: Hackers with a higher preference for analytic-rational information processing are more successful in their hacking activities.

H2: Hackers with a lower risk propensity are more successful in their hacking activities.

H3: Hackers with a higher preference for analytic-rational information processing estimate the risks involved in hacking to be higher.

H4: Hackers with a lower risk propensity estimate the risks involved in hacking to be higher.

H5: Hackers with a higher preference for analytic-rational information processing take longer times to prepare for their hacking attacks.

H6: Hackers with a lower risk propensity take longer times to prepare for their hacking attacks.

H7: Hackers with a lower risk propensity engage in fewer hacks.

All seven hypotheses are examined in the present study. The preference for rational thinking and the risk propensity of hackers are assessed and their influences on the overall hacking success, estimated risks, average preparation times, and the total amount of hacks are measured.

The Importance of Situational Adjustments

Different offenses provide different benefits to offenders and are committed with specific motivations. Some hackers engage in hacking merely to satisfy their curiosity about how different computer systems and setups work and to find out about their vulnerabilities, while others hack for financial gain, peer recognition, or personal revenge. Still others deface websites to voice their political opinions or to express their general antipathy with the host or the content of the site. The variables weighed by offenders and the factors considered in their decision making vary accordingly. Decision-making processes are fundamentally influenced by varying situational variables and the situational factors involved in different crimes vary greatly. For example, the situational factors involved in the intrusion into a computer system are substantially different from those in a bank robbery or the snatching of a purse (De Hann & Vos, 2003).

The above mentioned circumstance demands that situational choice decision models and flowcharts are not studied in abstract, general terms, but rather are developed specifically for the respective crimes that they are supposed to explain. This notion disqualifies wide legal categories such as cyber-trespass or cyber-theft as an appropriate basis for event models because they encompass too much variation with regard to types of offenses, offenders, methods, and goals. Consequently, such categories have to be broken down into more specific categories that permit models with greater precision and validity.

The increased validity of more specific event models, however, inescapably confines the generalizability of such models. Creating separate models for hacks that are

committed with different network mapping tools, for example, is probably not a fruitful approach, unless the researcher wants to study exactly those differences. Narrow models based on situational assumptions so specific that their applicability becomes restricted to only a very few situations are of limited scientific value. The challenge in the creation of event models then becomes finding the right balance in the pay-off between validity and generalizability. Clarke and Cornish suggest guiding the specificity of models along practical considerations, namely whether drawing finer distinctions results in large enough collections of offenses to justify separate interventions. If the answer to this question is yes, the distinction should be made. If it is no, they recommend finding solutions for addressing the variety of crimes subsumed under the broader category (Clarke & Cornish, 2001, p. 26).

While this proposition does translate directly into testable hypotheses, it presents an important aspect to consider in the creation of theoretical models and flowcharts. In order to be able to better understand and predict behavior, researchers have to gain an understanding of the underlying decision-making processes, the motivations driving these processes, and the influential factors considered in them. They have to identify relevant motivations, desired outcomes, and situational variables. Once the influential variables are identified, researchers can then begin to examine their relative importance and their specific effects on the outcome of that decision-making process. Eventually, this line of research will produce path-dependency models that will help to explain and predict offender behavior and, in some cases, may even be able to prevent criminal behavior by proposing changes in the “choice-structuring properties” (Cornish & Clarke,

1987, 1989) of hackers that increase risks and efforts, reduce rewards, and remove excuses (Clarke, 1997; Piquero & Tibbets, 2002).

The Differences between Involvement and Event Decisions

The decisions to generally become involved in criminal activity and to commit a particular crime can and must be distinguished from each other. The decisions involved in the commission of a particular crime, referred to as event decisions, include considerations such as the selection of specific targets and of methods to reduce the risk of apprehension. In order to avoid detection, hackers might, for example, launch their attack from public Internet cafes, or through encrypted networks such as the I2P or the TOR networks.

Involvement decisions, on the other hand, refer to the general decision of becoming involved in criminal activity. The highly complex nature of such decision-making processes requires researchers to further subdivide the broad concept of involvement. Typically, rational choice theorists distinguish three different stages of involvement: (1) initiation, i.e. the onset of a criminal career when offenders begin to view criminal activity as a viable option to achieve their goals; (2) habituation, i.e. the procedural continuation of a criminal career and; (3) desistance, i.e. the point when offenders decide to discontinue their criminal career and to desist from future offending (Clarke & Cornish, 2001).

While the requirement to specify event decisions models for different types of crime seems to be obvious, the creation of separate involvement decision models for different stages and different types of crime is just as important. Involvement decisions

at different stages and for different crimes include varying social background factors, current situational circumstances, available (il-)legitimate opportunities, and differing estimates of costs and risks. Not only are the skills and contacts required for certain types of crimes different, but it is also reasonable to assume that offenders distinguish the severity and immorality of different crimes. The fact that a person attempts to gain unauthorized access to a computer system, for example, does not imply that this person has no moral objections against stealing or destroying information that is stored on it. Clearly, one model size does not fit them all. Instead, models need to be tailored to the type of crime and the stages of involvement in order to provide a more precise picture of relevant factors.

The Three Different Stages of Involvement

As was mentioned before, the broad concept of involvement requires further distinction between different phases because the stages of initiation, habituation, and desistance are based on different variables and factors. According to the rational choice perspective, these variables and factors belong to three different groups: (1) background factors, e.g. bio-psychological factors, socialization, and learned experiences; (2) current life circumstances, e.g. routines and lifestyles; and (3) situational variables, e.g. momentary needs and motives and (il-)legitimate opportunities.

The rational choice perspective hypothesizes these three groups of factors to be disparately influential for the three phases of involvement. Background factors are thought to exert the greatest influence in the initiation phase because they predetermine the person's skills, experiences, morality, and friendships, as well as their socioeco-

nomic statuses. During the habituation phase, the criminal activity and the gains and risks associated with it gain gradually higher relevance for the current life circumstances, and the immediate life circumstances, in turn, become the most influential factor for decision-making processes. As involvement in criminal activity continues and becomes more and more habitual, mounting negative experiences and increasing realization of the potential costs involved, in combination with certain changes in the offender's life circumstances, could eventually lead them to desist from offending. Regardless of the stage of involvement, however, the rational choice perspective puts great emphasis on the importance of contextual variables that are present in a specific decision situation. Situational variables such as opportunities and inducements or needs and motives ultimately tip the scales toward the commission of or abstention from a particular crime.

In proposing different models of the factors likely to be involved in hacking-related decision-making processes, Figures 1 – 3 show the three different involvement stages of a hacking career, while Figure 4 presents a model of the concrete event decision to launch a particular hacking attack. All four models are close modifications of the models proposed by Cornish and Clarke. They adjust Cornish and Clarke's models by translating them into the context of hackers and by introducing some factors specific to hacking, but they assume the same general developments within and between the different phases as the original rational choice perspective models. In addition to criminogenically relevant factors, the models also list computer proficiency related factors because, unlike other types of cybercriminal activity, successful hacking requires the offender to have extensive computer knowledge and skills.

Figure 1 displays the variables influencing the initial decision to become involved in this particular activity. The starting points of the model are the various background factors commonly identified by criminological theories as being influential to the decision to engage in criminal behavior. These factors shape the values, attitudes, and behaviors which predispose people to consider committing crimes. It is important to bear in mind, however, that some of these background variables have to be treated with caution because hackers (and cyber-criminals in general) exhibit some characteristics that are substantially different from the attributes of the majority of other criminals, as was stated in the previous chapter (Wall, 2001). While demanding caution, this problem is at least partially alleviated by the circumstance that, within the rational choice perspective, these factors are considered to be only indirectly influential. They exert their influence solely through their influences on judgments and perceptions in the decision-making process.

The second box includes the various learning experiences the potential offender has had in his or her life with regard to the decision at hand. Accumulated prior learning experience is very important because the action alternatives evaluated in the decision-making process are interpreted against the background of these experiences, and some alternatives are enabled only through specific prior learning experiences. Successful computer hacking, for example, requires substantial knowledge of computers, networking structures, methods of attacks and attack tools, potential exploits, and programming skills. Without these prerequisites, hacking is probably not a fruitful course of action and will result in the mere execution of basic prewritten scripts, if it is considered as an action alternative at all.

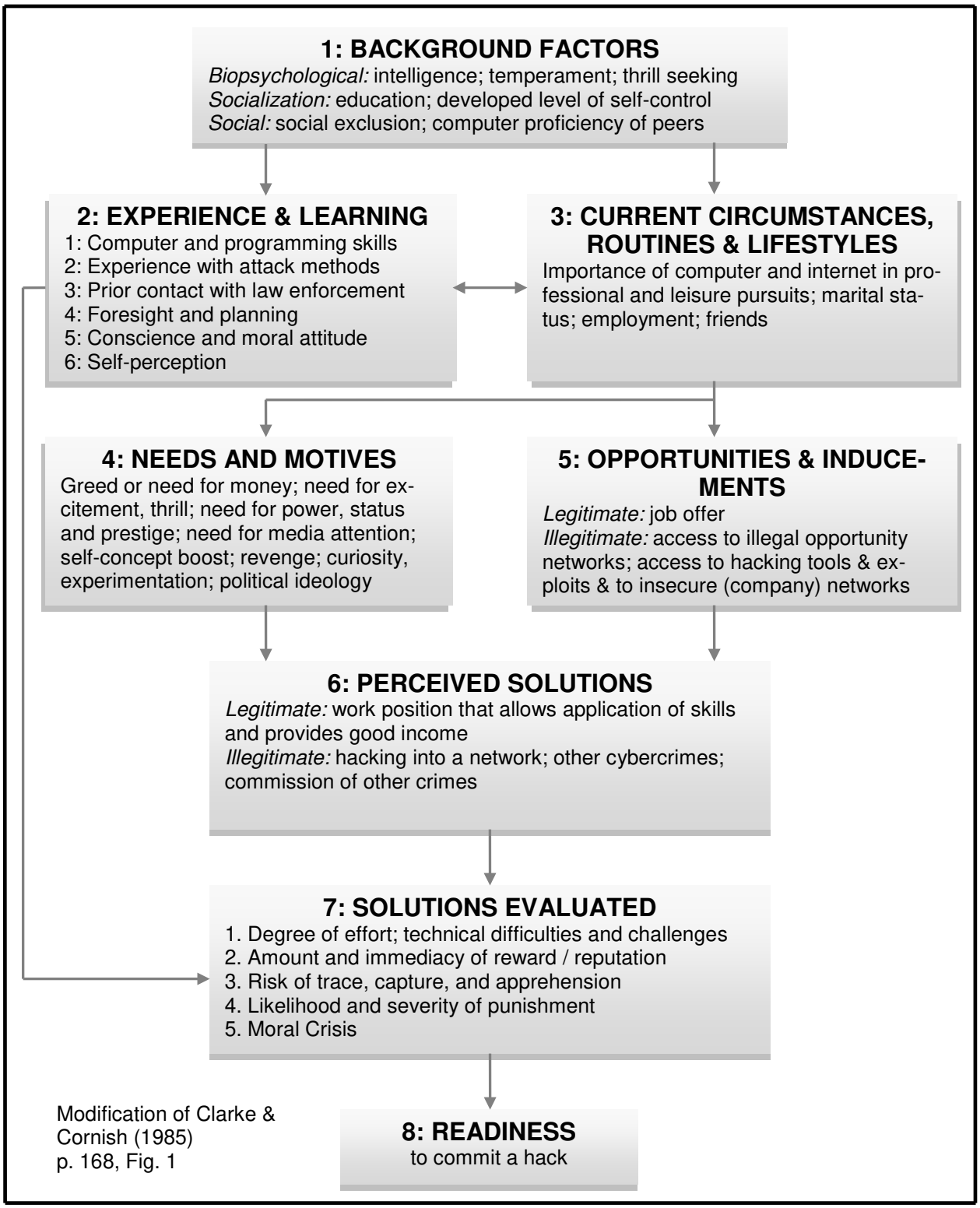

Figure 1: Model for the Initiation of Hacking

Box three lists the current life circumstances of the person. These circumstances are relevant to the decision-making process because they structure the needs and motives displayed in box four as well as the perceived opportunities and inducements to fulfill the needs and attain the desired goals shown in box five. The perceived solutions to reach the desired goals listed in box six differentiate between legitimate and illegitimate alternatives. Each of the alternatives under consideration is then evaluated in terms of the valued utility they provide and the risks and types of potential costs they include. The actor further estimates the probability that either the benefits or the costs will be the actual outcome.

Some versions of rational choice theory reconstruct this decision-making process in great detail and with mathematical equations. They assign expected utility values to benefits and costs and multiply these values with the probability assigned to them. The predominant and most attractive alternative, the one that yields the highest expected utility, is the one that is hypothesized to be invariably selected—otherwise the actor would not act in accordance with his or her own subjective rationality, and the primary proposition of rational choice theory would be violated. Cornish and Clarke's rational choice perspective does not attempt to reconstruct the decision-making process with mathematical equations, but it shares the principal assumption of the more elaborate models that show that the most beneficial alternative is selected once the decision-making process is concluded and the actor has selected the one alternative he or she deems most beneficial.

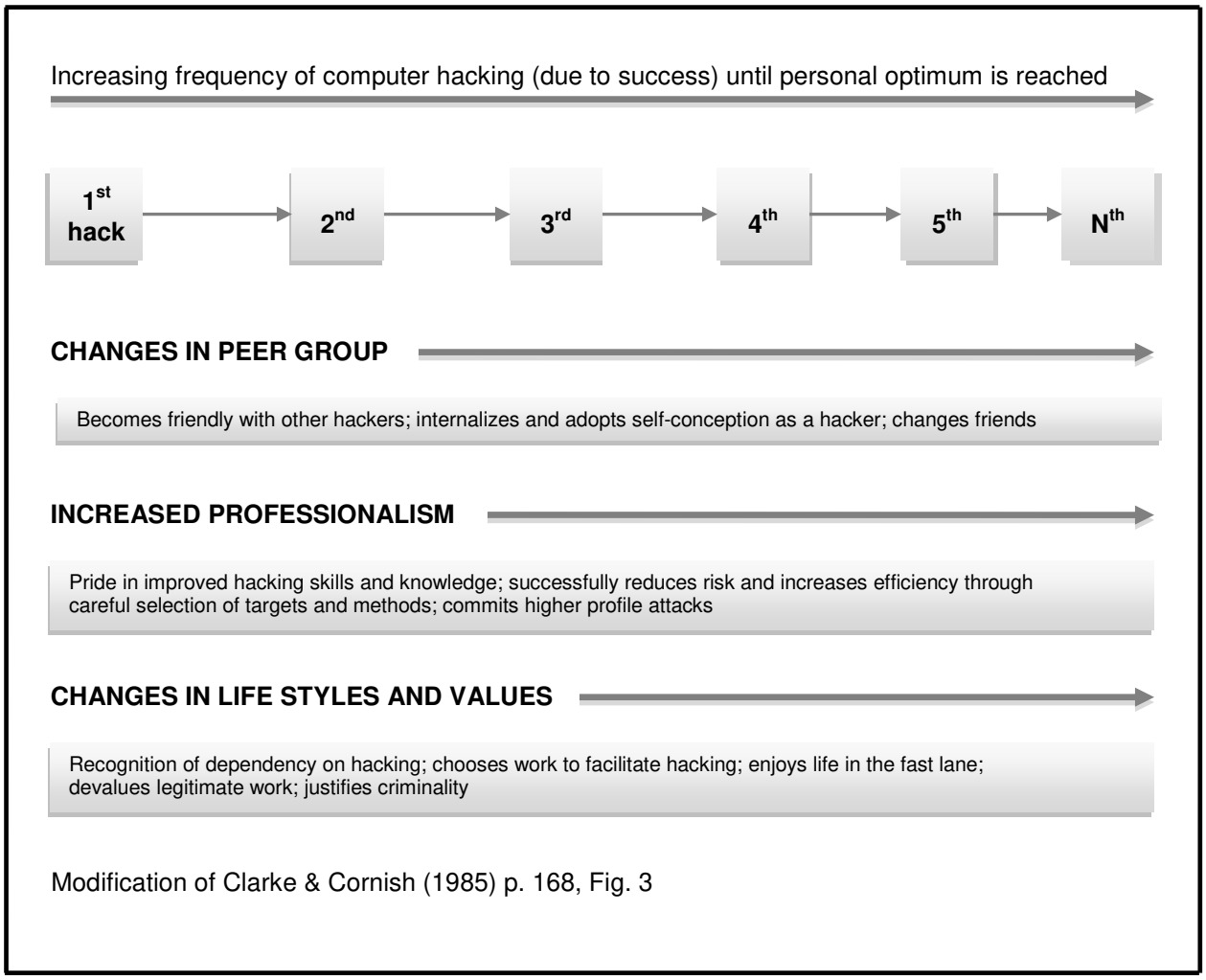

Figure 2: Model for the Habituation of Hacking

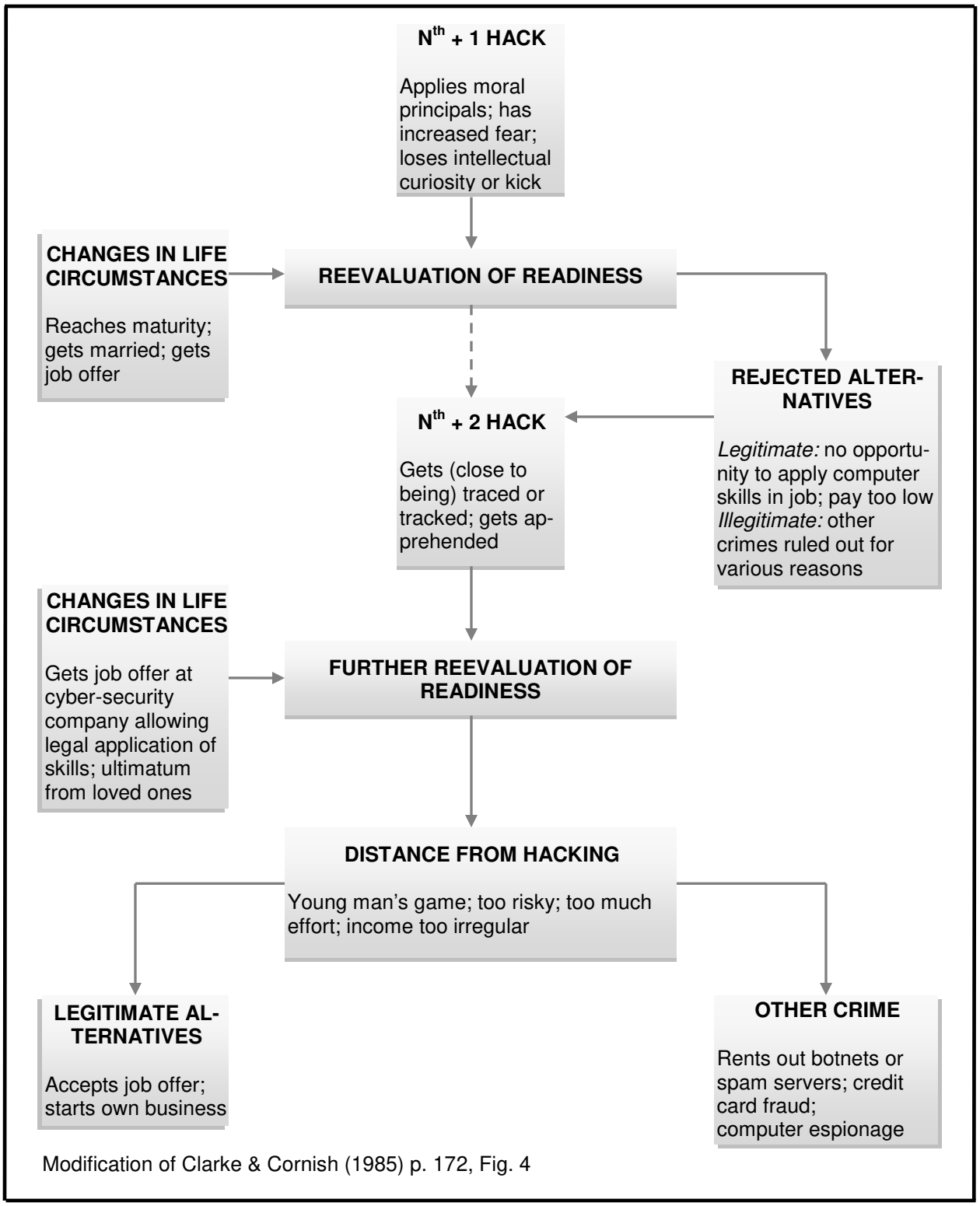

Figure 3: Model for the Desistance from Hacking

In the process of habituation, shown in Figure 2, the central influence on decision making gradually shifts from background variables to the rewards of successful engagement in the criminal activity and the influences this engagement has on the current life circumstances. The offender often changes peer groups and becomes closely involved with other persons sharing their interests, because these persons can provide him or her with valuable information and other resources. The self-perception as a hacker then becomes internalized and the person takes pride in his or her improved skills and knowledge. Throughout the successful habituation process, the methods of attack become increasingly sophisticated, which also reduces the perceived risk of apprehension. Offsetting the risk reduction of increased professionalism, on the hand, is the probable selection of higher profile targets by more experienced hackers. Higher profile targets are more attractive to seasoned hackers because they promise more interesting information, more reputation, higher financial gains, or just a greater challenge and thrill. However, higher profile targets also bear a higher risk and make activities riskier, not safer. Whether Cornish and Clarke's theoretical assumption of a decrease in the subjectively estimated risk potential over the course of a criminal career is valid when applied to hackers is presently unclear and will be examined in this study.

Cornish and Clarke's model further predicts that over the course of a criminal career, offenders justify their increasingly criminal and deviant behavior by employing "techniques of neutralization" (Sykes & Matza, 1957). Applied to hacking, such techniques of neutralization could, for example, be the presentation of the behavior as an expression of the hacker's commitment to the free flow of information, or as resistance to political authoritarianism and corporate domination.

Towards the end of the habituation phase, background factors play only a remote and unimportant role in the decision-making process. As shown in Figure 3, the offender begins to consider desistance once negative experiences have been made, life circumstances have changed, and/or new legitimate and promising opportunities have opened up.

The Reconstruction of Crime Events as a Decision Sequence

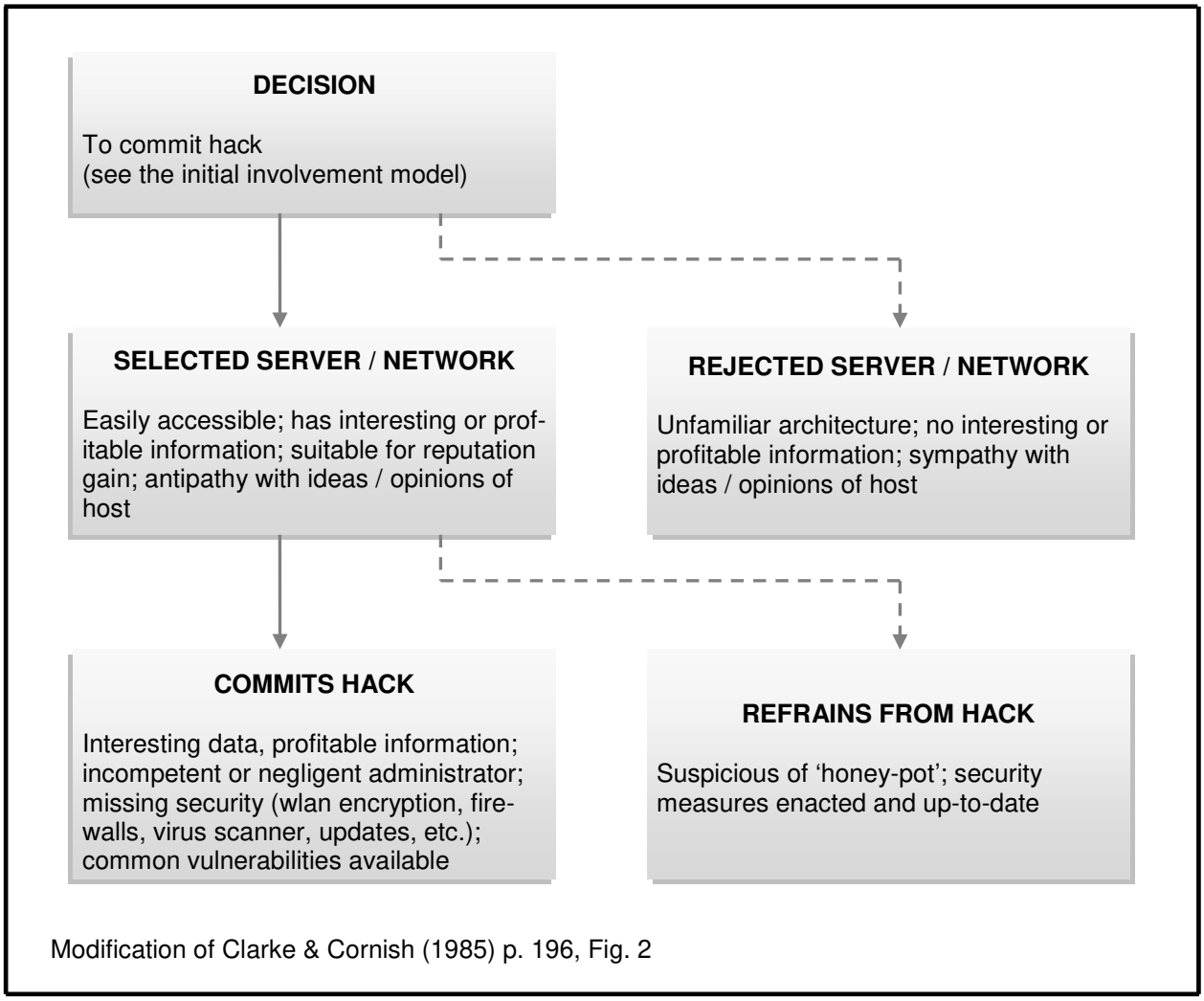

Figure 4: One Stage of the Crime Event: The Selection of a Target

Many criminological theories reduce the actual crime event to the selection of a suitable target. Rational choice theories, on the other hand, view the crime event itself as a series of decision-making processes that merely begin with the selection of a target. This seems to be the more accurate perception because oftentimes, crime events unfold in unforeseen ways and the offender has to adjust accordingly.

Figure 4 displays the hacker's selection of a suitable target for the attack. However, this selection is only the first in a complex process towards the completion of a successful attack. In 1994, Cornish borrowed the concept of crime scripts (Cornish, 1994) from cognitive psychology and introduced it into criminology. The crime scripts approach attempts to reconstruct the detailed procedures used by offenders in the commission of their crime step-by-step. It is a well-suited theoretical approach for the reconstruction of many different types of criminal behavior (Cornish & Smith, 2003). Its application to hacking, however, is a difficult undertaking because, unlike many crimes that are rather simple acts and similar to other mundane everyday activities (Gottfredson & Hirschi, 1990), hacking is an oftentimes highly complex and non-linear activity and a single hacking event can involve many different procedures and routes of action. Thus, the detailed reconstruction of the scripts involved in hacking presents not only a difficult theoretical challenge, but an even greater challenge for operationalizing and testing. Tests of such models can probably be best assessed through findings from crime science studies or with cognitive interviews of individual hackers. Cognitive interviewing is based on a technique called protocol analysis (Ericsson & Simon, 1980, 1984). During a protocol analysis, subjects are asked to verbalize their thoughts as they perform a particular action or solve a problem. These verbalizations are then recorded

and evaluated by the researcher. Repeated cognitive interviews during various types of hacking attacks will eventually produce theoretical models that accurately reflect the complexity involved in this activity.

The primary goal that the present study seeks to achieve is not to conduct individual case studies of hacking events, but to generate quantifiable insights into the hacking community and to assess the general importance of the various factors that, according to the rational choice perspective, are related to the involvement in hacking activities. Hence, the analysis focuses on testing the seven hypotheses that were stated earlier in this chapter. In addition to the influence of rationality and risk propensity on the conduct and outcomes of hacking activities, the analysis examines the relevance of several factors that the three involvement models consider to be important. It will be up to future crime science or protocol analyses to complement the insights that are generated by this study with more specific reconstructions of the crime scripts in hacking events.

To accomplish the goal of producing generalizable results, the study utilized a survey as measurement instrument. A survey format was selected because surveys are the social research method that is best suited to produce quantifiable findings. This feature renders them the most appropriate method for obtaining information about the distributions of sociodemographic characteristics and motivations of hackers, and for examining the pertinence of main factors of the three models shown above. The details of the research design and process as well as the individual items that were included in the questionnaire are specified in the following chapters.

CHAPTER SIX:
RESEARCH DESIGN

The goal of the present study is to test all of the hypotheses stated in the previous chapter and, given the exploratory nature of this project, to also generally examine the sociodemographic characteristics of the hacker community. To achieve these goals, the research project was designed to produce quantifiable results that are more representative and can be generalized to a wider target population than previous qualitative case studies of hackers (Jordan & Taylor, 1998; Taylor, 1999). A survey was developed and used for data collection (Boudreau, Gefen, & Straub, 2001), because surveys are the one data-collection method particularly suited to produce quantitative results that can be generalized to other members of the population of interest and oftentimes even to other similar populations (Newsted, Chin, Ngwenyama, & Lee, 1996).

Even though network administrators (D'Arcy, 2007), software developers (Lakhani & Wolf, 2003), and victims of cybercrimes (L. A. Gordon et al., 2005, 2006), for example, have all been the subject of several survey-based research projects in the past, no such survey-based study has been conducted on hackers so far. No study exists in the current cyber-criminological literature that allows scholars to draw conclusions about any larger population of hackers. Accordingly, the specific details and distributions of the hacking community continue to remain largely unknown. The aim of the present study is to undertake this task and to begin filling the remaining gap in the criminological literature on hackers and the hacking community by providing the first quantifiable insights into the hacking underground.

The Difficulty of Sampling Hackers

Although important to achieve, the realization of this study is challenged by a variety of difficult methodological obstacles. Most importantly, the quantitative nature of this research project demands that the problem of obtaining a sample that is reasonably representative of any larger hacker population is resolved. Two main characteristics of the hacking community, in particular, make the process of gathering a representative sample of hackers a difficult undertaking. First, partly due to their oftentimes illegal activity, hackers form a hard-to-reach and hard-to-identify, sealed off and mostly hidden underground community. Second, they present a rather rare population. Both of these circumstances present unique challenges for the sampling process. They require that researchers find a method for establishing contact with a representative sample of target subjects who are relatively small in number, decentralized, concerned about protecting their real identity, and who interact primarily through specialized online communication channels.

One potential solution to this problem is the utilization of some form of snowball sampling technique, in which a few active hackers who are known to the researcher recruit other subjects from their acquaintances for the study. The drawback of utilizing snowball samples is that they are confronted with the crucial problem of study subjects not being selected from any larger sampling frame. Dependent on the underlying network structures of the participating respondents, this circumstance subjects snowball samples to several uncontrollable biases (Groves et al., 2004). While some systematic snowball sampling techniques, such as respondent-driven sampling, are designed to

partially alleviate this problem (Heckathorn, 1997), no snowball sampling technique offers any remedies capable of eliminating coverage error. Consequently, these techniques do not permit accurate estimates of the representativeness of the population of interest.

Overcoming the representativeness problems associated with snowball samples is a difficult challenge when studying underground target populations because for these populations, no lists of eligible subjects are available. Hence, the researcher has to select a sampling method that allows the construction of a sampling frame which simultaneously minimizes the systematic undercoverage of eligible subjects and the inclusion of ineligible subjects (Groves et al., 2004). The difficulty of this particular methodological challenge is probably part of the reason why no quantitative study of hackers has been conducted so far.

In the case of hackers, two principle solutions are conceivable for this problem. One possible solution is to access the communication channels typically utilized by hackers. Such a study could attempt to advertise links to the survey on public hacker message boards and then draw its participants from members of the boards. Again, the problematic aspects of this method are evident. First, it would suffer from several shortcomings generally associated with Internet-based surveys. Unlike traditional methods of establishing contact with respondents, such as random-digit dialing in telephone surveys or sending surveys via mail, researchers have no direct access to the population within an online environment. Consequently, the sampling frame of Internet surveys remains a principal issue (Couper, 2000). The vagueness of the sampling frame entails other problems. For example, it severely limits the possibility to estimate nonresponse

rates (Couper, 2000), which, in the case of Internet-based surveys, are typically higher than those achieved with traditional recruiting methods (Matsuo, McIntyre, Taomazic, & Katz, 2004). Despite these problems, such an approach should not be generally discarded solely because of its sampling-frame related issues. As Gosling and colleagues point out, their Internet study, although perhaps not exactly representative of the population in general, nevertheless compared favorably to other publications with regard to all major sociodemographic characteristics (Gosling, Vazier, Srivastava, & John, 2004).

An additional set of problems confronting this approach is related to the environment in which respondents fill out the survey. In the case of online surveys, this environment is completely out of the researcher's control or influence. Problems resulting from self-selection, multiple submissions, non-serious responses, and dropouts are more severe because Internet surveys are completely self-administered and do not permit any ad hoc interaction between participant and interviewer. Hence, it is more difficult for the interviewer to recognize and correct problems of comprehension or intentional mischief (Porter & Whitcomb, 2003; Reips, 2002). This circumstance heightens the possibility of individual participants negatively impacting the quality of the results in online surveys (Nosek, Banaji, & Greenwald, 2002).

Particularly in the case of studies on hackers, the principal problems of Internet-surveys are likely to be further exacerbated. Many hackers are generally suspicious about the authenticity and trustworthiness of information they retrieve online. For the researcher, this implies that the difficult task of establishing the necessary trust without personal contact becomes a crucial challenge. Failure to convince hackers to trust the research project will cause many potential participants to refuse taking the survey or to

intentionally provide false information. Combined, all of these problematic aspects severely question the validity of the results yielded by this sampling approach.

An additional set of sampling-related problems of Internet-based surveys arises from the circumstance that their samples include only members of particular message boards, not hackers in general. Two aspects of this limitation are particularly problematic. Many message boards serve as discussion forums for specialized topics and are interesting only to fractions of the hacking community (e.g. http://sla.ckers.org/forum for web application security). Equally important is the circumstance that many of the more popular boards such as “The Phoenix Project” or “Hacker’s Den88” are typically consulted by lesser skilled beginners who use them for basic advice and guidance. Both of these aspects are likely to introduce systematic sampling biases because they lead to an underrepresentation of higher skilled hacking experts.

An alternative approach is to field the survey during an occasion when larger numbers of hackers meet in person. Each year, several hacker conventions take place in the United States (e.g. BlackHat, ShmooCon, DefCon, ToorCon, or PhreakNIC) and around the world (e.g. Chaos Communication Camp in Germany, CanSecWest in Canada, PacSec, SysScAN, and Hack in the Box in Asia, or even PakCon in Pakistan). Fielding a survey at such a convention presents the researcher with the opportunity to contact more seasoned experts and hackers who are involved enough to undergo the efforts and costs involved in attending a convention. While eliminating many of the problems associated with Internet-based surveys, researchers following this methodological approach have to keep in mind that all main hacker conventions have a distinct profile. Like Internet-based message board samples, they also attract only parts of the hacking

community. Consequently, studies based on samples of attendees of hacking conventions are also subjected to limitations regarding the generalizability of their results.

This circumstance holds two implications for research projects following this approach. First, researchers have to carefully consider several sampling-related criteria when selecting a convention. The world's largest annual convention DefCon, for example, has a reputation of drawing a large crowd of predominantly young and generally less experienced hackers who mainly attend the convention to have a good time with like-minded people. In contrast, other conventions draw more experienced security experts who are interested in the latest security-exploit developments, while others, like the BlackHat convention, even charge several thousands of dollars for attending advanced seminars in what the BlackHat organizers term "offensive security." In order for a convention to draw a sample of attendees who are most representative for the hacker community, it has to address a broad spectrum of topics and attract a wide variety of hackers with different security-related interests.

Second, the interpretation of the results has to take this sampling-related limitation into consideration. The fact that hacker conventions offer the most precise sampling frame for researchers does not imply that this convention-based sampling frame is equivalent to the target population of hackers in general. Strictly formulated, the findings of such a study can only be generalized to the greater population of hackers who would potentially attend the particular conference.

Despite the inevitable restriction regarding the generalizability of the results, this methodological approach is nonetheless better suited than snowball or Internet samples because of the strengths it offers in managing the task of sampling hackers. Most im-

portantly, it provides researchers with a delimited sampling frame. Surveys fielded at a particular convention can also serve as a point of reference to which future surveys that are fielded at different conventions can compare and contrast their results to. Eventually, such a comparison of results from different conventions will provide estimates that closely reflect the distributions within the diverse hacking community. For the present study, this approach presented a viable opportunity to gain the first general insights into an underground community that remains largely unknown. Because it is the least problematic sampling method and the one most likely to generate generalizable results, this methodological approach was chosen.

The ShmooCon Convention

The survey for the current research project was fielded during the 2008 ShmooCon convention in Washington D.C. The ShmooCon convention was selected because its profile closely matches the selection criteria outlined above. Since its first convening in 2004, ShmooCon has developed into one of the largest annual conventions worldwide. Today, it ranks among the most popular conventions, and it is attended by both U.S. and international hackers and security experts. In addition, it has one of the most diverse programs that is attractive to a wide variety of hackers (Grecs, 2008). The convention is commonly announced as an “annual East Coast hacker convention hell-bent on offering an interesting and new atmosphere for demonstrating technology exploitation, inventive software and hardware solutions, as well as open discussion of critical information security issues” (HackWire, 2004).

The 2008 convention was held over the weekend from Friday, February 15 to Sunday, February 17 in the Marriott Wardman Park Hotel in Washington D.C. After the official opening remarks on Friday afternoon, various speakers started the convention with presentations on a number of different topics ranging from “Intercepting Mobile Phone/GSM Traffic” to “Forensic Image Analysis for Password Recovery” and “Hacking the Samurai Spirit” to “New Countermeasures to the Bump Key Attack.” The main event on Friday was a keynote address given by Dr. Edward W. Felten, a highly renowned professor of Computer Science and Public Affairs at Princeton University and the founding Director of Princeton’s Center for Information Technology Policy.

The main program on Saturday and Sunday was divided into the three general sections “Build It!,” “Break It!,” and “Bring It On!.” In each of the three sections, expert speakers gave presentations on a broad variety of topics. The primary target audience of the “Build It!” section consisted of network administrators and other security experts. The section covered several topics of general interest to this audience, among them “They’re Hacking Our Clients! Why are We Focusing Only on the Servers?,” “Practical Hacker Crypto,” “Using Aspect Oriented Programming to Prevent Application Attacks,” “Hacking Windows Vista Security,” or “Path X: Explosive Security Testing Tools using XPath.”

The “Break It!” section, on the other hand, included presentations covering a variety of aspects related to the act of breaking into computer systems and networks. The section was geared towards black hat hackers and penetration testers alike and contained presentations entitled “Virtual Worlds – Real Exploits,” “Smarter Password Crack-

ing," "VoIP Penetration Testing: Lessons Learned," and "Malware Software Armoring Circumvention."

The third section "Bring It On!" covered topics generally related to the lives of hackers. The presentations in this section included titles such as "When Lawyers Attack! Dealing with the New Rules of Electronic Discovery," "The Geek and the Gumshoe or Can Mathematics and Crimes?," "You Must Be This Tall to Ride the Security Ride," "Legal Issues for Bot-net Researchers and Mitigators," or "How do I Pwn Thee? Let Me Count the Ways." Before the final closing remarks on Sunday afternoon, the main agenda of the convention ended with a large panel discussion "On the Social Responsibility of Hackers" that involved convention organizers and speakers from all three sections. Combined, the three main sections and the surrounding presentations and discussions addressed a broad variety of hacking and security-related topics that ranged from purely technical topics to sessions providing hackers with practical advice for coping with the problems and challenges in a hacker's life.

In addition to the expert speaker presentations in the three sections, the convention offered several other activities and competitions. Participants in the various hacking contests, for example, had to go on a virtual treasure hunt and gather clues and hints that were hidden all over the convention. Even the red laser engraved acrylic punch card badges that attendees received upon registration displayed different dot patterns of PDP-8 machine code that, if combined, led to other clues as part of one contest. The progress of the contestants in the hacking arcades was made public in real time by a projection of their advancement on one of the hallway walls. The winner of each contest was rewarded with prizes in the form of gaming consoles and, most importantly, the

recognition from peers. Prizes were also offered for the winners of the lock picking competition in the “Lock Picking Village” and the three first places in the “Hack or Halo” ego-shooter video gaming tournament. Other events during the convention involved several live-streamed online video feeds and interviews with prominent hackers as well as a Saturday night party in a nearby dance club.

The unconventional name of the convention was explained during the opening remarks. The ShmooCon conference received its name from the concept of so-called “shmooballs.” As part of the registration package, each attendee received a soft rubber stress ball the size of a tennis ball. All participants were explicitly instructed to throw this ball at the speaker when, during a presentation, they felt that the speaker made a mistake or did not know the material of the presentation well enough. The act of throwing the shmooball then entitled the thrower to voice their objections or to correct the speaker. In making this concept a central aspect of the convention, the ShmooCon organizers attempted to break down the hierarchies between speaker and audience and to solicit input from all experts in the audience. By doing so, they also demonstrated their adherence to the democratic ideas of the original hacker community. In a humorous demonstration of how the shmooball concept is intended to work, some of the staff members assaulted the opening speaker during his explanation of the shmooball concept with a self-made shmooball canon that fired a large magazine of balls across the auditorium at him.

Aside from the shmooball concept, several other organizational details implemented the creeds and convictions of the traditional hacking community. The application process, for example, was designed so as to give all interested persons the same

chance of obtaining an admission ticket. The tickets were sold exclusively online. The sales events took place on three different occasions on a first come, first serve basis. The sale of tickets was restricted to only three occasions because the number of admissions was limited to 800 attendees and, according to the convention organizers, the demand for tickets vastly exceeded their available number. The structure of the organizational team was itself organized in a strictly non-hierarchic, democratic fashion. All suggestions were due for approval and implemented only after they obtained a majority of the vote. Furthermore, the organizers underwent great effort to solicit detailed feedback from the attendees and, thereby, include them in the improvement process for future conventions.

Summarizing, it can be recapitulated that the conceptual layout of the 2008 ShmooCon convention made it an ideal candidate for the present research project. Its main program was designed to be inclusive and to address the interests of a wide variety of hackers. Its agenda combined a mixture of serious discussions of latest security issues and several events to entertain attendees, thereby making the conference interesting for hackers of all different backgrounds and skill levels. Before the survey was fielded during the conference, however, several steps were taken to ensure its appropriateness and its success as a scientific measuring instrument.

The Pretest and IRB Approval

Boudreau, Gefan, and Straub (2001) emphasize the need for every survey instrument to be pretested as a preliminary step that prevents unanticipated encounters during the fielding of the final version of the survey. Therefore, a pretest of the initial

draft of the survey instrument was conducted with a convenience sample comprised of six self-proclaimed hackers known to the researcher. Each of these testers volunteered to participate in the pretest. They received a copy of the initial draft along with some general instructions and information about the purpose of the study. The general instructions asked them to provide feedback about the design of the survey with regard to three aspects: (1) the suitability and appropriateness of the individual items and answer categories in general, (2) their estimate of the suitability of individual items to address the larger research questions, (3) the appropriateness of the content and structure of the instrument for the intended target population and measuring situation.

The long geographical distances between the pretest participants, who are residing in different countries, did not permit the researcher to conduct personal debriefing sessions. Instead, the panel members were asked to provide detailed written feedback after their completion of the survey and to return their comments via email. The feedback received from this pretest focused primarily on revisions of the wording and was aimed at eliminating potential ambiguities in some of the hacking-related questions. It also included some suggestions for minor changes in the provided standard answer categories. While there was general agreement among the reviewers on the general suitability and appropriateness of the items included in the survey and on the exhaustiveness of the provided standard answer categories, one particular item received negative feedback and was therefore excluded from the final survey. All six participants reported that answering the item “What does the term hacking mean for you?” was disproportionally time-consuming since it consumed almost as much time as the remainder of the survey.

In a subsequent step, the revised version of the survey draft was reviewed by two experienced survey researchers on the sociology faculty at University of Central Florida. Aside from providing a second scrutiny of the appropriateness of the survey tool and the unambiguousness of the individual items, this expert assessment was also used to ensure the appropriateness of the survey as a scientific measurement instrument and to examine the content validity of the items, many of which were developed specifically for the present study and had not yet been validated. Based on the recommendations of these experts, some modifications and refinements were implemented in the final version of the questionnaire. In particular, the wording of a few individual items was revised and some items were rearranged. There was agreement among the reviewers on the importance of all main sections of the questionnaire, on the appropriate length of the measurement tool, and on the suitability of the included items to address the intended dimensions of the underlying concepts. Thus, the results of these pretests suggest that the questionnaire was well designed for the research project and possessed adequate validity.

Following the pretest of the questionnaire, the research proposal was submitted to the University of Central Florida Institutional Review Board (IRB) for approval. The submitted proposal materials consisted of the study questionnaire, an informed consent document, and an online application that detailed the various aspects of the study to the IRB reviewer. The informed consent form (see Appendix B) served as an identification of the researcher. It also informed prospective participants about the details of the project they are going to participate in and granted confidentiality and anonymity. To ensure the highest possible degree of anonymity, the documentation of consent was

waived on the consent form. The study was exempt from a full board review because it recruited no vulnerable populations and posed only minimal risk for participants since it did not ask respondents to reveal any specific self-incriminating information. Only a few formal stipulations were requested by the IRB reviewer in the initial review, and the study received IRB approval after the requested changes had been implemented.

The Data Collection Process

Once IRB approval was obtained, a formal request for permission to field the questionnaire during the convention was submitted to the organizers of ShmooCon. Although this request was received positively, the organizers expressed their main concern as brokers for the community of protecting their attendees' privacy, and they asked for the submission of additional identification materials. Among the requested identification was the curriculum vita of the principal investigator, the contact information of a study supervisor, a detailed research proposal, the documentation of IRB approval, and a statement that the survey was for research purposes only and involved no commercial or governmental institutions or organizations.

Once all these materials had been submitted and reviewed, the study was approved and the organizers of the convention even offered to announce the survey project as an integral part of the convention in the opening remarks to build trust among the attendees. The announcement of the study in the opening remarks included a PowerPoint slide that informed attendees about the research project and its IRB approval as well as a personal introduction of the principal investigator. This introduction by the organizers proved to be of invaluable help for the acceptance of the study. Many res-

pondents immediately recognized the researcher from the opening remarks when they were asked to participate in the study.

Furthermore, the organizers of the convention provided a table in the central hallway between conference rooms and several chairs for participants to take the survey. The survey table was in an ideal location next to the sponsor booths and between presentation rooms. Whenever attendees walked from one presentation section into another, they passed by the study table. Placed on the survey table were copies of the questionnaire, consent forms, large University of Central Florida printouts, poster-sized prints inviting attendees to “be part of the first survey on hackers,” business cards of the researcher, and Snickers candy bars as incentives to participate. Convention attendees passing by were verbally approached by the researcher and invited to participate in the study. They were told that the survey referred to hacking as the unauthorized intrusion into computer systems, networks, or website servers and they were asked to participate only if they had ever committed such an intrusion. Attendees who indicated that they worked as penetration testers were asked to only participate if they had ever invaded a computer system outside of a contractual agreement and instructed to only refer to these intrusions in their answers. Penetration testers and other attendees who reported to have never committed such a hack were told that the survey did not pertain to them and were dissuaded from taking the survey.

Approximately one-third of the approached attendees were rejected because they had never committed an unauthorized computer intrusion. Most of the rejected attendees were penetration testers who reported to have always followed a strict ethical code. A smaller fraction of the rejected attendees had simply never attempted a com-

puter intrusion, either because they had just recently become interested in hacking or because they attended the conference with their significant other who is actively hacking. A total of 164 questionnaires were distributed among qualified attendees. Most of the persons who agreed to participate in the study filled out the questionnaire on site. Some, however, asked to take it with them and fill it out at a more convenient situation. Of the 164 distributed surveys, 129 were returned to the researcher, 124 of which were filled out completely and included in the analysis of the study. Thus, the response rate of completed and returned surveys was 75 percent and an estimated 25 percent of all eligible attendees were included in the study. The large fraction of sampled units and the high response rate can be attributed to the personal interest many hackers displayed in the survey project and to the trust the official announcement of the study had helped to build.

CHAPTER SEVEN:
THE SURVEY INSTRUMENT

The survey instrument of the current study was designed to test all of the hypotheses stated in the third chapter. In particular, it assessed the main phases in the careers of hackers as proposed by the rational choice perspective and examined the extent of rationality in their involvement and event decision making. In addition, it also measured the general distributions of sociodemographic characteristics within the hacking community.

At the beginning of the questionnaire, a small introductory section welcomed the respondents, thanked them again for their willingness to participate in the study, and provided a brief introduction of the researcher and the purpose of the study. It also reassured respondents that the survey is strictly noncommercial and for dissertation research purposes only, that there are no institutions or organizations involved or affiliated, and that their participation in this project is voluntary, anonymous, and confidential.

The measurement instrument itself consisted of a total of 72 items in three main sections. The first section gathered detailed information about the various phases of the respondents' hacking careers. It embodied items pertaining to the initiation of the hacking activity, its habituation, and the eventual desistance from hacking. It further assessed several other details of the respondent's hacking activity, including a variety of involved decisions and motivations. Given the exploratory nature of this research project, many items in this first section offered open-ended "Other" answer categories in

addition to the answer options provided. The answers recorded in these open “Other” categories were included as string variables in the dataset. Several of the items also permitted respondents to give multiple answers. All answer options listed for these items were coded as separate dichotomous variables.

The second section of the survey instrument consisted of questions measuring the degree of risk propensity, rationality, and faith in intuition in the respondents’ decision-making processes. The main reason for the assessment of these three personality traits was to allow the survey instrument to test all of the hypotheses that were derived from the rational choice perspective in chapter three. The operationalization of theoretical hypotheses concerning the influence and degree of rationality in decision-making processes presented a principally difficult methodological challenge. Typically, such assumptions are measured with either fictional scenarios of nearly real-life decision-making situations (Clarke & Cornish, 2001; Finch, 1987; Harrington, 1996; Kerlinger, 1986) or with social psychological scales (Clarke & Cornish, 2001; Kerlinger, 1986). The decision to operationalize the three personality traits with social psychological scales in the present study was made because this assessment format better fitted the setting in which the survey was fielded. It was less demanding to merely ask respondents to indicate their agreement to some general statements than to have them read through several fictional scenarios before answering questions. Moreover, this measurement technique also reduced the overall length of the survey and the time needed for its completion. Further lengthening the survey with scenarios might have decreased the attendees’ willingness to participate, given that the survey was already eight pages long and took about 15 minutes of the time they spent at the convention.

All items in this second section were taken from well-established scales that were abbreviated to keep the overall length of the survey within reasonable limits. The decisions about which items to include were based on statistical and conceptual considerations. Items were selected according to their item-to-total correlations and their factor loads on the respective underlying dimension. To maintain construct validity despite the shortening of the scales, items were also selected based on their ability to measure different aspects of the underlying concept. All items were anchored on appropriately labeled seven-point Likert-type scales. Seven-point scales were chosen over five-point scales because they allow for finer distinctions in the measurement of the variables (Sommer & Sommer, 2002). Another advantage of seven-point scales is that increasing the scale end points from five to seven also tends to increase the ability to reach the upper limits of reliability (Krosnick & Fabrigar, 1997; Nunnally, 1978).

The third section concluded the survey instrument with measures of basic sociodemographic information. The items included in the three parts of the survey instrument, which can be found in Appendix A, are presented in greater detail in the following sections.

The Measurements of General Hacking Activity

The first item in the survey asked respondents to indicate whether they are currently actively hacking. Two dichotomous answer categories, “Yes” and “No,” were provided and respondents who answered with “No” were instructed to think back to when they were still hacking when answering the subsequent questions. The rationale behind the placement of this item at the beginning of the questionnaire was to differentiate be-

tween active hackers and respondents who had been hacking at one point in their lives but had desisted from hacking in the meantime or had given up any illegal hacking activities to become penetration testers.

The items measuring the various aspects of the respondent's hacking career were organized in chronological order. The first set of questions examined the onset of the hacking activity. Respondents were asked to indicate how old they were when they first became interested in hacking and to also provide the motivations that initially got them interested in this activity. The motivations listed as standard answer categories for this question were derived from the existing literature on hackers (Taylor, 2000, 2004; Thomas, 2002; Yar, 2005a) and arranged according to their assumed importance (Yar, 2005a). The listed motivations were "Intellectual Curiosity," "Excitement, thrill, fun," "Experimentation," "Status and prestige," "Financial gain," "Peer recognition," "Political ideology," "Media attention," "Protest against corporations," "Self-concept boost," "Feeling of power," "Personal revenge," and an open-answer category "Other (specify)." A second item then asked participants to indicate which of these motivations had been their primary one.

Further examining the onset phase, the following item then asked participants to indicate the length of the time frame between their initial interest in hacking and their first actual hack. The purpose of this item was to provide a frequency measure that permitted comparisons to later stages of the respondent's hacking career and, thereby, allowed additional measures of whether the activity has indeed become more intensified. The answer categories for this item gave respondents the choice to enter their an-

swers in days, weeks, months, and years. All answers were later recoded into days to provide a unified scale for the corresponding variable in the dataset.

After the examination of the initial interest phase, the survey shifted to questions about the details of the first actual hack the respondents had ever committed. Again, participants were asked about their specific motivations to commit this first hack. The answer categories listed for this question were the same as for the previous question about the motivations that had sparked the initial interest in hacking. The motivations for the first hack were measured separately from the motivations that initially got respondents interested in hacking because this separate measurement provided an indication of the consistency between the two. Thereby, it also allowed an assessment of the relative importance of situational factors in the decision to commit the first hack. For example, a person could become interested in hacking out of intellectual curiosity but then decide to launch a hacking attack in an attempt to take personal revenge.

The next question then asked respondents to specify the type of target they selected for their first hacking attack. The set of answer categories for this item distinguished between single hosts, networks, and websites and between private, corporate, non-profit, and governmental entities. Again, the item also included an “Other” category that allowed respondents to specify any other type of target. Further detailing the aspects of the target, the subsequent item asked participants to report the criteria their target selection was based on. The answer options given for this item were “Easy access,” “Interesting information,” “Profitable information,” “Reputation gain,” “Antipathy,” and again “Other.”

Two additional items were included in the questionnaire to explicitly assess the role financial motivations and considerations played during the onset of the hacking career. The first asked participants whether they were employed at the time they committed their first hack. The answer options for this item were “Yes, full-time,” “Yes, part-time,” and “No.” The second item directly asked respondents whether “economic profits [were] a motivation at all.” The answer categories for this item were “Yes, an important one,” “Yes, but not important,” and “No.”

To provide a more detailed assessment of the first hack ever committed by the participants, the survey asked them to indicate the methods they used in their first technical intrusion. The item referred to the first hack as the first technical intrusion because it was intended to measure only the technical methods employed in the first hack. The term “technical intrusion” basically denotes all attempts to subvert exploitable system or network defaults, holes, bugs, or passwords. It excludes other methods that can be used in a hack, such as social engineering methods. Specifically, respondents were instructed to mark all technical methods they had used in their first hack from a list of 24 of the most common technical intrusion methods (Kanellis, Kiountouzis, Kolokotronis, & Martakos, 2006). The methods listed as answer options for this item were arranged in a sequential order from reconnaissance tactics over different ways to gain access to a computer system to methods for covering up any potential traces. The reconnaissance tactics included in the list were “Footprinting,” “Ping sweeping,” “DNS zone transfer,” “Whois,” “Network mapping,” “Port scanning,” “Versatile scanning tools,” and “Vulnerability scanning.” The methods of gaining access to computer systems contained were “RPC port/end-point dump,” “Packet sniffing,” “Session hijacking,” “Grinding pass-

words," "Password cracking," "Password theft," "Directory traversal/climbing," "Buffer overflows," "Format strings," "Resource mismatches," "CGI," "Root shell/kits," and "Key-loggers." The list ended with three common methods for covering up any potential traces: "Spoofing," "Bouncing," and "Source routing." Even though this list basically covered the methods most commonly used by hackers (Kanellis et al., 2006), the number of possible attack tactics is far greater. Thus, the answer categories were again complemented by an open-ended "Other" category. Since it cannot be assumed that all readers are familiar with all different hacking techniques, the skill-level they require, and the type of target they are usually used against, the different methods are briefly introduced in the Glossary.

The assessment of individual hacking methods was included for a twofold purpose. The primary reason was to provide a measurement of the prevalence of several known hacking tactics and methods. Currently, no quantitative estimate of the popularity of different hacking methods exists in the literature, because the victimization surveys conducted on the issue thus far can assess the methods that are being used in hacking attacks only indirectly and incompletely. Some methods simply leave no traces on the target machine. Others can be rendered undetectable to victims or even cyber-forensics by several potential circumstances. For example, many reconnaissance methods leave no traces on the target computer and, oftentimes, efforts to cover up traces succeed in rendering the detection of intrusion methods impossible.

The second purpose of the inclusion of item measuring the employed hacking methods was to also provide a potential assessment of the level of technical skills the respondent had when they launched their first hacking attack. Some hacking methods

require a much more advanced skill level, whereas others can be performed by merely executing common software tools. Thus, the item also provided an indirect proxy measure of the skill-level during the onset of the hacking activity. The decision to include an indirect measurement of the respondents' skill level at the beginning of their hacking careers rather than a direct measurement was made in an attempt to avoid the potential self-perception and social-desirability biases introduced by a direct measurement. While suited to avoid such biases, conclusions about the skill-level of the attacker have to be drawn cautiously from this indirect assessment because the selection of a particular method is not solely dependent on the skill-level of the attacker. The decision to use a particular method is also influenced by the type of target and the specific vulnerabilities of a particular target. Directory traversals, for instance, are attack methods that are used primarily for website attacks, but not for attacks on computer systems or networks. Furthermore, conclusions about the skill-level of the attacker have to be drawn with caution, because some of the attack methods denote categories that can subsume different attacks of varying difficulty.

The next set of questions on the questionnaire asked hackers about their hacking career in general. The questions in this part were broken down into three different hacking activities that were measured separately. The questionnaire distinguished between technical intrusions, so-called "Wetware" social methods, and the distribution of malicious code. Wetware is a term commonly used among hackers and computer programmers. It is an analogy to software, but refers to the act of programming a brain, as opposed to computer code. Six common wetware methods were listed as answer op-

tions: “Social Engineering,” “Deception,” “Bribery,” “Shoulder surfing,” “Impersonation,” and “Dumpster diving.” The six methods are briefly introduced below.

Social engineering basically denotes all attempts of hackers to establish and subvert trust relationships with victims or to predict their behavior. Once a trust relationship is established, the attacker tricks the victim into revealing information or performing an action, such as a password reset, for example, that can then be used in the attack. A subcategory of social engineering methods are so-called reversed social engineering methods, in which attackers use their expertise to induce their victims to reveal sensitive information when seeking their help and advice. Deception is a method similar to impersonation, but demands a higher commitment than the latter. Whereas an impersonation can be as simple as sending an email pretending to be somebody else, deception typically refers to attempts to gain inside access to a network in order to be able to launch an attack from behind its firewall. Shoulder surfing and dumpster diving are two other popular social methods that directly exploit the oftentimes careless behavior of targets. Shoulder surfing describes an attack method in which the hacker simply monitors the moment the victim types passwords or other sensitive information on their keyboard. Once the login information is known, the hacker can exploit the user account without having to worry about any counter measures such as firewalls or intrusion detection systems because they can no longer distinguish between the legitimate user and the attacker. Similarly, dumpster diving, a slang term for searching through the target’s garbage, is a simple and oftentimes legal method to gain valuable information because many people dispose of sensitive information without destroying it first. Bribery is probably the easiest way to hack wetware, but it is not as common in developed western na-

tions as it is in developing countries. More profound bribery attempts than simple direct cash payments usually align the financial interests of the target with those of the hacker.

Whereas technical intrusions and social engineering methods are the two attack methods typically associated with hackers, a third category of attacks, the distribution of malicious code, was also included in the questionnaire. This method of attacking computer systems is not necessarily limited to only hackers, but is oftentimes also used by other cyber-criminals such as email phishers or spammers. Nevertheless, it was included in the questionnaire to measure hacker attempts of gaining control over target computers by distributing malicious code. The answer categories given for the question "Have you ever distributed?" were "Trojan Horses," "Adware/Spyware," "Viruses/Worms," "Spam/Phishing mails," "None of the above," and "Other." Readers unfamiliar with these types of malicious codes can find brief descriptions in the glossary accompanying this text.

The engagement in each of the three types of hacking methods was measured with three items asking respondents to: (1) estimate how often they had attempted these types of hacking methods in their life, (2) indicate the frequency with which they engaged in those types of methods, and (3) provide an approximation of their success with these methods. The answer categories provided for the frequency measurement were attempts per weeks, months, or years. All answers were later recoded into days to obtain a unified interval-scaled variable. The estimated success rates of technical intrusions and social methods were measured on scales of ten percent increments ranging from zero to 100 percent. The success rate of malware distributions was not measurable this same way because the success of malicious code distributions primarily de-

pends on how many computers become infected with that code. Thus, the success with malware distributions was measured with a seven-point Likert-type scale ranging from 1"Not at all" to 4 "Somewhat" to 7 "Very" successful.

Further examining the continuation of the respondents' hacking careers as proposed by the rational choice perspective, the next set of items asked respondents: (1) whether they changed friends and peers since their first hack to include other hackers; (2) whether they believe they improved their skills since their first hacking attempts; (3) whether their hacking activity has become more frequent since their first hacking attempts; and (4) whether their motivations had changed since their first hacking attempts. The three answer options given for these items were "Yes, very much," "Yes, somewhat," and "No." The item measuring the frequency of hacking attempts further distinguished between the two answer options "No, it's the same" and "No, it's less frequent." A last item in this set asked respondents to specify their currently predominant motivation for hacking in an open format.

The respondents' selection decisions of targets for hacking attacks were measured with five items. The first two items asked whether respondents had changed targets since their first attacks and whether their targets had become higher profile targets. Again, the answer options "Yes, very much," "Yes, somewhat," and "No" were given. The third item then detailed the type of currently preferred targets. Like the answer options given for the question about the target of the first hacking attempt, the answer categories provided for this item distinguished between single hosts, networks, and websites, and between private, corporate, non-profit, and governmental entities. Again, an

open answer category was provided to allow respondents to specify any other types of targets.

The last two target-related items asked about the criteria influencing the selection or rejection of a particular target. The criteria provided for the question “What are your current selection criteria for targets?” were the same as for the item measuring the selection of the target in the first hacking attack: “Easy access,” “Interesting information,” “Profitable information,” “Reputation gain,” “Antipathy,” and “Other (specify).” The criteria listed for the question “What might be a reason for you to reject a potential target?” were “Unfamiliarity with architecture,” “No interesting information,” “No profitable information,” “Sympathy with host,” “None of the above,” and again “Other (specify).”

The set of questions following the target-related items interviewed participants about various aspects of their hacking attacks. Respondents were asked whether they had changed their methods and tactics since their first hack and what their currently preferred methods and tools are for the different stages of a hack. For the item measuring the currently preferred methods, the six main stages of a hack “Reconnaissance,” “Gaining access,” “Persisting,” “Propagating,” “Paralyzing,” and “Covering up” were listed and respondents were instructed to enter their preferred methods and tools for each of the main phases. They were then asked whether they follow a persistent pattern in all their hacks or vary their methods and software tools between hacks. The answers to both questions about the variability in methods and tools were recorded on seven-point Likert-type scales ranging from 1 “Very persistent pattern” and “Always same tools” to 7 “Vary a lot.”

The section detailing the aspects of the respondents' current hacking activity then ended with an item measuring the methods they employed to remain anonymous. The answer options provided for this question were "Spoofing," "Bouncing," "Source routing," "Proxies," "TOR, I2P, etc.," "Tunnels, Covert channels," "War driving," "Public access points (e.g. Internet cafes)," and "Other (specify)." All eight anonymizing methods utilize different techniques to hide the offender's true identity. Spoofing is a tactic hackers commonly use to pretend they are somebody else. The disguise is accomplished by entering the wrong source IP addresses in the TCP/IP headers of data packets. Bouncing is a method that is similar to spoofing. In the case of bouncing, the hacker uses proxy servers or computers to relay, or bounce, their requests to the attacked machines. Thereby, the impression is evoked that the attack originated from the proxy, when in fact it was only channeled through it. In the context of computer networks, proxies denote gateways that relay one Internet session to another. Proxies cannot only be used for bouncing techniques, but some proxy servers are even specifically designed for anonymizing purposes. The use of such proxies makes the real source of data packet untraceable. Source routing denotes a technique that allows a sender of data packets to specify the route these packets take through a network. Source routing can be used in hacking attacks to reach otherwise unreachable targets through intermediate computers that are connected to the target. TOR (The Onion Router) and I2P (Invisible Internet Project) are both open source projects that are similar in that they enable their users to communicate anonymously on the Internet. Tunnels and covert channels, on the other hand, are methods used by hackers to circumvent firewall protections and evade intrusion detection systems. Lastly, war driving and public access points are two

methods to access the Internet anonymously through other persons' private or public networks. In the case of war driving, the hacker drives through an area in a moving vehicle with a WiFi-equipped computer and searches for open or weakly secured wireless networks that are then used as Internet access points.

The last set of questions in this first part of the questionnaire examined possible doubts the respondents had about their hacking activity and their readiness to desist and end their hacking careers. The first item in this last set of questions asked respondents whether hacking is a source of income for them. The answer options given for this item were "Yes, the main," "Yes, but not the main," and "No." In addition to providing an explicit measure of financial considerations, this item also enabled the researcher to compare the relevance of financial considerations during the onset and the later stages of the hacking activity. The item was followed by the direct question about whether the respondent had ever thought about quitting hacking. The three answer options for this item were "Yes, often," "Yes, a few times," and "Never." An additional item was included to measure the reasons for thoughts about quitting. The reasons listed for this item were "Involved risk," "Involved effort," "Income too irregular," "Fear of detection," "Fear of apprehension," "Fear of prosecution," "Legal alternatives," and "Other (specify)."

The first part of the questionnaire ended with seven items measuring the respondents' estimation of risks involved in their hacking activity. The first risk-related item asked them whether they are more or less afraid of being traced, tracked, or apprehended now than when they began to hack. The four answer options for this item were "More afraid," "Less afraid," "Unchanged," and "I was never afraid." Respondents were then asked to estimate the time they usually invested in preparation, planning, consid-

eration of routes of action, and the selection of techniques and tools. The answers were recorded in hours, days, weeks, and months and were entered in the dataset in hours with one day equating to eight hours. An additional measure of the development of carefulness was provided by the item “Do you spend more or less time for planning today than when you started to hack?” The three answer options for this item were “More time today,” “About the same time,” and “Less time today.”

The next risk-related items then asked respondents to estimate the risk they run of being detected and of being apprehended during or after a hack. Both items were recorded on seven-point Likert-type scales ranging from 1 “No risk at all” to 4 “Some risk,” to 7 “Very high risk.” The second to last item in this section measured the percentage of attacks the respondents had aborted because they were afraid of being detected. The percentage of aborted attacks was again measured on a scale of ten percent increments between zero and 100 percent. The first section of the questionnaire concluded with asking respondents whether they were more focused on potential rewards or potential risks during their hacks. The risk versus rewards focus question was measured on a seven-point Likert scale ranging from 1 “Only on rewards” to 4 “Balance both” to 7 “Only on risks.”

The Measurements of Risk Propensity and Rationality

The second part of the questionnaire consisted of items from different scales designed to assess the influence of three personality factors. In particular, the three scales measured the respondents’ risk propensity as well as their preference for rational versus heuristic or experiential-based thinking styles. In an attempt to limit the overall

length of the survey, each of the three scales was abbreviated to five items. All items in this second section were worded as general statements, and respondents were instructed to indicate how much they agree or disagree with these statements on seven-point scales ranging from 1 “Strongly disagree” to 7 “Strongly agree.”

The decision to measure general risk propensity with a scale instead of a single item was based on findings by MacCrimmon and Wehrung (1990), who reported that the concept of risk propensity is too broad to be accurately captured with a single item. The five items measuring risk propensity were taken from different scales and slightly modified for best thematic fit. The first item “I always try to avoid situations involving a risk of getting into trouble” was modified from a scale developed by Dahlback (1990). The second item, “I always play it safe even when it means occasionally losing out on a good opportunity,” was adapted from Gomez-Mejia and Balkin’s (1989) “willingness to take risks” scale, which is an advancement of the original scale developed by Slovic (1972) and the modifications introduced by Gupta and Govindarajan (1984). The remaining three items were taken from Dulebohn (2002), who developed them to measure general risk propensity and who reported a Cronbach alpha of .73 for this three-item scale. The second item “I am rather bold and fearless in my actions” was reversed to prevent biases introduced by “acquiescence” response strategies of participants who give superficial answers because they want to get through questions quickly (Krosnick & Fabrigar, 1997).

Two other scales were included to assess the degree to which respondents generally rely on their rationality versus their intuition when making decisions. All items in the rationality and the faith in intuition scales were taken from the latest version of the

Rational-Experiential Inventory (REI) scale (Pacini & Epstein, 1999). The REI is a well established and supported measurement instrument for rational versus heuristic thinking styles. Today, considerable evidence exists in the social psychological literature for its construct validity (Epstein, 2003; Epstein, Pacini, Denes-Raj, & Heier, 1996; Handley, Newstead, & Wright, 2000; Pacini & Epstein, 1999).

The full version of the REI consists of 40 items in two main scales measuring the preference for analytical-rational or intuitive-experiential information processing. Each of the main scales is further divided into subscales of self-assessed effectiveness and of engagement in both thinking styles. More precisely, rational effectiveness refers to the confidence persons have in their logical reasoning, whereas rational frequency or engagement refers to the pleasure derived from rational thinking (Handley et al., 2000). Conversely, experiential ability measures the confidence in relying on personal intuitions and experiential engagement measures the enjoyment of using intuition as the basis of one's decision making. The internal consistency reliabilities are reported with .87-.90 for the two REI scales and .79-.84 for the four subscales (Epstein, 2003). The full version of the REI scale was abbreviated in the survey. The questionnaire contained five items from each of the two REI scales. Three of the five items in each scale were taken from the ability subscales and two from the engagement subscale. The selection of items followed the criteria that were outlined earlier in this chapter.

The Measurements of Sociodemographics

The questionnaire concluded with some measurements of basic sociodemographic characteristics in the third section. Respondents were first asked to indicate

their sex and to enter their year of birth. They were then asked to identify the last grade they completed. The answer categories provided for this question were “None, or grades 1-8,” “High school incomplete (grades 9-11),” “High school graduate (grade 12 or GED certificate,” “Business, technical, or vocational school AFTER high school,” “Some college, no 4-year degree,” “College graduate (B.S., B.A., or other 4-year degree) ,” and “Post-graduate training/professional school after college (Master’s degree or Ph.D.).”

The racial and ethnic background of the participants was assessed with two items. The first item asked whether the respondents are “of Hispanic or Latino origin or descent, such as Mexican, Puerto Rican, Cuban, or some other Spanish background.” The second item then asked them to indicate their race. The answer categories provided for this item were “White,” “Black,” “Asian,” and “Other mixed race: (specify).” The marital status of respondents was measured with the question “Are you married, living as married, divorced, separated, widowed, or never been married.” The last two questions on the survey asked “Are you now employed full-time, part-time, retired, or not employed for pay?” and “Are you also a full- or part-time student.” The survey concluded with thanking the respondents for their participation and wishing them a nice day at the conference.

CHAPTER EIGHT:
METHODS AND RESULTS

The analysis conducted in this research project addressed all the study goals that were outlined in the previous chapters. Aside from examining the distributions of sociodemographic characteristics within the hacking community, it also specified the rational choice perspective models for the continued involvement in hacking by measuring the shifting importance of various motives as well as several other hacking-related aspects. Furthermore, it tested all hypotheses raised in Chapter 5 by investigating the effects of varying degrees of rationality and risk propensity on hacking-related decisions.

Given the exploratory nature of the research project, the first section describes the distributions of sociodemographic characteristics in a univariate analysis. Descriptive statistics are also used to identify the relative importance of several hacking-related factors. In the second section, the validity and reliability of the three personality scales are briefly examined, and the scales are transformed into indices. These indices are then used to test the hypotheses from Chapter 5 in several additive multivariate linear regressions.

The Sociodemographic Composition of the Sample

The sociodemographic characteristics displayed in Table 1 show a vastly skewed gender distribution among hackers. Only seven of the 124 participants (5.6 percent) were females. The wide gender gap revealed in this study confirms other reports that describe hacker communities as being predominantly male (Adam, 2004; Taylor, 1999).

Table 1: Sociodemographic Characteristics of Sample Respondents

Variable	N[1]	%[2]
Sex		
Male	117	94.4
Female	7	5.6
Age[3]	120	30.6 (6.7)
Education		
None, or grades 1-8	0	0.0
High school incomplete	4	3.2
High school graduate	7	5.6
Vocational school	2	1.6
Some college	30	24.2
College graduate	47	37.9
Post-graduate Master's or Ph.D.	34	27.4
Race		
Hispanic descent	3	2.4
White	116	93.5
Black	2	1.6
Asian	5	4.0
Other	1	0.8
Marriage status[4]		
Never married	63	50.8
Living as married	17	13.7
Married	43	34.7
Divorced	1	0.8
Employment		
Full-time	92	74.2
Part-time	22	17.7
Unemployed	10	8.1
Student status		
Yes, full-time	14	11.3
Yes, part-time	31	25.0
Not a student	79	63.7
Actively hacking		
Yes	97	78.2
No	27	21.8

[1] The total sample size is n=124.
[2] Percentages may not add up due to rounding.
[3] Measured in years, means reported (std. dev. in parentheses).
[4] Some categories were excluded because they yielded no results.

The general underrepresentation of women in all areas related to computing and information technology—except in office or administrative positions—has already received considerable scrutiny in the literature (Webster, 1996). Against this background, the vast domination of males in the hacking community is not surprising. However, the gender difference in this study exceeded even the discrepancies found in other areas of computing and information technology, in which women are estimated to account for 10 to 30 percent of participants (Zarrett & Malanchuk, 2005).

Taylor traces the absence of women in the hacking community, which he finds to be an "unexplained statistic," (Taylor, 1999, p. 32) back to what he sees as the fundamentally masculine nature of hacking. He describes the hacking culture as young, male, technology-oriented, and laden with factors that discourage women from joining. Among the factors listed by Taylor are social stereotyping, a masculine "locker room" environment, and a gender biased computing language (Taylor, 1999, p. 36). Adam goes one step further by describing the hacker culture as one that, despite the explicit egalitarianism expressed in the Hacker Ethic, is nevertheless characterized by a "frontier masculinity," a "Wild West brand of masculinity," and a deeply rooted misogyny displayed by men who hide behind the anonymity of the Internet and associate "technology with desire, eroticism and artificial creation" (Adam, 2004, p. 6). The data collected in the present study confirmed the existence of a substantial gender gap, but it did not include any additional attitude measurements with regard to gender. Hence, it is not possible to confirm or reject any of the explanations mentioned above. Nevertheless, some of the elements identified by Adam and Taylor were clearly visible during the convention. For

example, some attendees wore T-Shirts with labels such as “Penetration Expert” or other print designs that connected technology with expressions of male sexuality.

Aside from the large gender gap, the data also displays a heavily skewed race distribution. Over 93 percent of the hackers in the sample were White, a fraction that vastly exceeded the percentage of Whites in the U.S. population. Another noteworthy finding in the race distribution is the fact that Asians were the largest minority in the sample. While the low cell count of all minorities in the present study did not permit accurate generalizations of this finding, this result again reflects the racial distributions in most IT professions (Zarrett & Malanchuk, 2005). A common explanation for this finding is the particular prevalence of positive attitudes toward math, science, and computer-related occupations among Whites and many Asian cultures (Bement, Ward, Carlson, Frase, & Fecso, 2004).

The age distribution of the convention attendees shows a much higher mean value than the one suggested by the common notion of the prototypical hacker as a juvenile delinquent teenager (Yar, 2005a). It is reasonable to assume that the higher average age in this study of ShmooCon convention attendees was caused by the sampling frame of this particular research project. The profile of the ShmooCon convention was geared more toward security experts and computer professionals than to teenagers who pursue their hacking interests merely as a leisure-time hobby. Thus, while the distribution in this particular sample is certainly not enough evidence to falsify any claims that the majority of hackers are teenagers, nevertheless, it indicates that the hacking community is by no means limited to only teenagers. To the contrary, it involves many mature security experts and many seasoned hackers who pursue their hacking activity in a

professional manner. The data clearly show that hacking is not just a 'young man's game.' The oldest active hacker in the sample was 52 years old and reported to have been hacking for close to three decades.

The professionalism of most respondents was also reflected in their educational attainments. Ninety percent of the hackers in the present sample had at least some college education, and about one-fourth of them reported to have obtained a Master's or Ph.D. degree. Moreover, about one-third of all respondents were enrolled either as full-time or part-time students. An examination of the four cases with an incomplete high school education revealed that most of them were young participants (between 18 and 19 years old) who also reported to be full-time students. These four cases were most likely high school students who had not yet graduated.

The high fraction of students in the survey sample is particularly surprising when considering the fact that over 90 percent of all respondents were also employed. About three-fourth reported to be employed full-time and an additional 18 percent were part-time employees. The high employment rate was probably part of the reason why more than double as many respondents indicated to be part-time students than full-time students. When asked about their marital status, about half of all respondents said that they were never married. A significantly smaller fraction, only about one-third of all participants, reported to be married.

In short, the sociodemographic characteristics that were sampled in this study paint the picture of a hacking community that is predominantly male, White, and comprised of highly educated members. They also work regular jobs and are oftentimes also studying but appear to be hesitant to engage in serious relationship commitments.

The Descriptive Statistics of Continued Involvement

The control item at the beginning of the questionnaire asked participants whether they “are currently actively hacking.” Almost 80 percent of the respondents answered this question with “yes.” A brief examination of the remaining 20 percent revealed that most of them were very active former hackers who had given up their hacking activities in the meantime. The result obtained from this control item allows the conclusion that the goal of the present study, which was to sample persons with actual hacking experiences and not just persons who are merely interested in computer-security related issues, was indeed accomplished.

The Initiation Phase

Some of the most interesting questions about the initiation phase of hacking are (1) what exactly sparked the initial interest in hacking, (2) what led hackers to commit their first actual hacking attempt, and (3) at what age did they do so. All three questions relate to main components of the initiation model as proposed by the rational choice perspective, and all three questions were addressed in the present study. The results show that many hackers became interested in hacking even before their early teenage years. One person reported that he was only nine years old when he first became interested in hacking. While this respondent was the youngest, he was no exception. Table 2 shows that the first peak in the initial interest distribution was as early as 12 years. Twenty percent of all respondents reported to have already been interested in hacking by that age. The median of the distribution was at 15 years, and the mean at 16 years.

Table 2: Motivations for Interest in Hacking and First Hack

Variable	N[1]	%[2]
Age interested in hacking[3]	124	16.0 (4.3)
Motive for initial interest[4]		
Intellectual curiosity	118	95.2
Experimentation	105	84.7
Excitement, thrill, fun	82	66.1
Feeling of power	26	21.0
Peer recognition	23	18.5
Self-concept boost	22	17.7
Status and prestige	19	15.3
Personal revenge	12	9.7
Other	7	5.6
Political ideology	6	4.8
Protest against corporations	4	3.2
Financial gain	3	2.4
Media attention	2	1.6
Primary motive for interest[4]		
Intellectual curiosity	74	59.7
Experimentation	21	16.9
Excitement, thrill, fun	15	12.1
Feeling of power	4	3.2
Other	4	3.2
Self-concept boost	2	1.6
Political ideology	2	1.6
Peer recognition	1	0.8
Personal revenge	1	0.8
Motive for first hack[4]		
Intellectual curiosity	91	73.4
Experimentation	84	67.7
Excitement, thrill, fun	56	45.2
Feeling of power	13	10.5
Peer recognition	10	8.1
Self-concept boost	10	8.1
Status and prestige	4	3.2
Personal revenge	6	4.8
Other	3	2.4
Protest against corporations	2	1.6
Financial gain	2	1.6

[1] The total sample size is n=124.
[2] Percentages may not add up due to rounding.
[3] Measured in years, means reported (std. dev. in parentheses).
[4] For better readability, the motives are rank ordered by importance.

The self-reported motives for the initial interest in hacking show that the majority of participants became interested in hacking because of “intellectual curiosity” (95 percent), “experimentation” (85 percent), and “excitement, thrill, or fun” (66 percent). A second set of motives revolving around self-expression and peer-recognition turned out to be of significantly lesser importance. Among these motives were “feeling of power” (21 percent), “peer recognition” (19 percent), “self-concept boost” (18 percent), “status and prestige” (15 percent), and “personal revenge” (10 percent).

Some of the motives that are oftentimes associated with hackers in media reports (Alexander, 2005) as well as scientific (Grabosky & Smith, 1998; Kilger, Arkin, & Stutzman, 2004) and governmental publications (Krone, 2005), on the other hand, played only a marginal role as initial interests. Among these motives were “political ideology” (5 percent), “protest against corporations” (3 percent), “financial gain” (2 percent), and “media attention” (2 percent). The results clearly demonstrate that motives associated with youth, boredom, frivolity, mischief, or curiosity are the main reasons for young persons to become initially interested in hacking. In contrast, only a very few respondents became interested in hacking because of political or financial considerations, or other motives with a stronger criminal intent.

A similar pattern emerged from the question about the single most important motive for the initial interest. Here, roughly four times more respondents (60 percent) answered with “intellectual curiosity” than with the next popular answer option “experimentation” (17 percent). “Media attention”, “financial gain”, “protest against corporations”, and “status and prestige,” on the other hand, were not mentioned at all and were excluded from Table 2.

Only five “Other” reasons were specified. Out of those, the desire to spy on a girlfriend, who the respondent believed to be cheating, was named twice. The other reasons were independence, learning of security, and playing pranks on friends. Overall, the few individual reasons that were given in addition to the list of standard answer options suggest that the list was comprehensive. The only item that should probably be included in the theoretical model and future measurements was spying.

The separate measure of the motives for the first actual hack produced roughly the same results as the item measuring the motives for the initial interest. The main difference between the two items was that the reasons for the first actual hack were more specific than for the initial interest. Accordingly, most respondents marked fewer motives, which resulted in lower percentages for all motives. The patterns between the different motives, however, were very similar to the ones emerging from the question about initial interests. Two noteworthy findings in the distribution of motives for the first hack were that “political ideology” was not mentioned by any respondent and that “financial gain” was a motive for only two respondents.

Aside from the motivations for the initial interest and the first actual hack, the survey also measured the length of the time span between these two events. The time measure was recorded in days in the dataset but is presented in more meaningful categories in Table 3. Interestingly, about one-third of all respondents committed their first hacking attempt already within the first week of becoming interested in hacking. Also, an additional 20 percent committed their first hack within the first month of becoming interested. This finding suggests that the initial interest of many hackers is not an abstract, intellectual enterprise, but a preparation for their first hack. It indicates that the initial in-

terest is guided by the intent to actually launch hacking attacks. Less than 50 percent were interested in hacking longer than a month before they actually attempted a hack. The longest reported time span in the sample was clearly an outlier (10 years). Table 3 displays the recorded time spans between initial interests and first hacks.

Table 3: Details of the First Hacking Attempt

Variable	N[1]	% [2]
Time span between interest and hack[3]		
Up to 1 week	45	36.3
Up to 1 month	23	18.5
Up to 1 year	31	25.0
2 to 10 years	25	20.2
1st target owner / type N (%)	N (%)	N (%)
	Single host	Network	Website
Private	50 (40.3)	29 (23.4)	4 (3.2)
Corporate	5 (4.0)	7 (5.6)	3 (2.4)
Non-profit	0	4 (3.2)	1 (0.8)
Government	1 (0.8)	1 (0.8)	0
1st target selection criteria		
Easy access	70	56.5
Interesting information	36	29.0
Profitable information	0	
Reputation gain	0	
Antipathy	7	5.6
Other	11	8.9
Employed when 1st hacked		
Yes, full-time	28	22.6
Yes, part-time	28	22.6
No	68	54.8
Economic profit a motive at all		
Yes, an important one	0	
Yes, but not very important	5	4.0
No	119	96.0

[1] The total sample size is n=124.
[2] Percentages may not add up due to rounding.
[3] Categories are not cumulative.

Table 3 further shows that the most popular targets of the first hack were single private computer hosts (40 percent) and private networks (23 percent). Corporate computers and networks were the second-most popular targets (4 percent and 6 percent). With regard to corporate targets, the relationship between single hosts and networks was reversed. More corporate networks were attacked than single computers. This difference is probably due to accessibility reasons. While many single private hosts can be located in unprotected wireless networks or public networks, an attack on corporate computers typically requires a preceding attack on the network in which the computer is located. Only one hacker selected a government host and network as the targets for his first attack. For all others, these targets were probably too risky and too high profile to be considered as a first target.

Most hackers selected their first target based on practical considerations. The majority of participants (57 percent) reported that the ease of gaining access was their primary selection criteria. About half as many chose a particular target because it offered interesting information (29 percent). Revenge or antipathy with the host played only a minor role as selection criteria. Only seven respondents attacked their targets because of personal dislike (6 percent). Some specifications of answers in the “Other” category (9 percent) revealed that some respondents counted attempts to hack their own computer system or network as their first hacking attempt. Future survey designs will need to be more explicit to rule out this interpretation of the question.

The answers to the selection criteria question again confirmed the irrelevance of commonly assumed motives in the initiation phase. None of the respondents attacked their targets in search for profitable information or because they were particularly suited

for gaining a reputation as a hacker. The finding that financial interests played hardly any role during the onset of hacking activity was also confirmed by the answers to the explicit question asking whether economic profits were a motive at all. Only five respondents (4 percent) said it played a minor role. The vast majority (94 percent), on the other hand, indicated that economic considerations or potential financial gains had nothing to do with their decision to start hacking.

The finding that a majority of respondents (55 percent) were unemployed when they first hacked is not surprising given the young age of most respondents when they started to hack. During their first hacks, most of them were still dependent teenagers with little or no income of their own. Despite little or no income, however, it is important to note that economic interests hardly played any role in the decision to engage in hacking activities.

The Popularity of Different Hacking Methods

Table 4 shows the popularity of the 24 different hacking attacks that were listed in the questionnaire. When interpreting the results, it is important to bear in mind that the corresponding item asked respondents only about attacks they had used in their first hack. Hence, the frequencies in Table 4 relate to only one single hacking event, not all hacking attempts over the course of a career. Despite the fact that the question referred to merely one single event, some of the attack methods were used by almost half of all respondents. The most popular methods were packet sniffing (49 percent), port scanning (47 percent), buffer overflows (47 percent), and network mapping (44 percent). Of the 24 answer options, bouncing was the only method that had not been applied by an-

ybody in the sample. The high frequency turnout of most items in the list, however, was a strong indication that the listing of methods in this study was appropriate.

The fact that only a few specialized methods were specified as answers in the "Other" category further suggests that the list was close to being exhaustive. Most of the methods specified in the "Other" category were antique methods that were popular in the 1980s and 1990s but have since become obsolete. The implication that the provision of standard answer options for this question had the disadvantage of systematically excluding outdated methods that older hackers used in their first attacks was reaffirmed by the verbal feedback from some of the older hackers. Nevertheless, the provision of standard answer categories for this question produced much better results than the relatively unsuccessful open-ended measurement technique that was used for the question about currently preferred methods and tools. Most respondents were hesitant to reveal their methods or tools and either skipped the question, or gave nondescript answers such as "custom tools." By way of comparison, they were much more willing to mark already provided answer categories. The differential success of the two measurement techniques suggests that future surveys should operate with standard answer categories for questions about preferred hacking methods because this question format minimizes the reluctance of many respondents to reveal this information.

The results shown in Table 4 further suggest that the description of most hacks as complex events with different phases is correct. Many hackers combined different reconnaissance methods with different intrusion and cover-up techniques. Two of the most popular reconnaissance methods were network mapping and port scanning. Oftentimes, these two methods were used in combination. After hackers had created a

map of the network and had located the target computer within that network, they then searched for vulnerable open ports as entry points to that computer system. Of the different methods to gain access to a system, the various techniques to obtain passwords were the most frequently used. These results suggest that the classic exploitation of password weaknesses remains popular among many hackers.

Table 4: Methods Used in First Hacking Attack

Variable	N[1]	%[2]
Methods used in 1st technical intrusion		
Footprinting	34	27.6
Ping sweeping	29	23.2
DNS zone transfer	7	5.8
Whois	36	29.0
Network mapping	54	43.5
Port scanning	58	46.5
Versatile scanning tools	29	23.2
Vulnerability scanning	45	36.3
RPC port/end-point dump	2	1.5
Packet sniffing	61	49.4
Session hijacking	18	14.5
Grinding Passwords	14	11.6
Password cracking	38	30.5
Password theft	36	29.0
Directory traversal/climbing	14	11.6
Buffer overflow	58	46.5
Format string	5	4.4
Resource mismatch	2	1.5
CGI	4	2.9
Root shell/kits	9	7.3
Keylogger	29	23.2
Spoofing	14	11.6
Bouncing	0	
Source routing	4	2.9
Other	26	21.0
Average number of methods (std. dev.)	5.0 (19.5)	

[1] The total sample size is n=124.
[2] Percentages may not add up due to rounding.
[3] Categories are not cumulative.

The Prevalence and Success Rates of Different Kinds of Attack Methods

Table 5, 6, and 7 list the prevalence and success rates for three different types of hacking attacks. While many persons think of hacking attacks as performed solely through technical means and exploits, they are in fact more diverse and oftentimes involve a combination of technical methods, social methods, and circulations of different kinds of malicious code (J. Erickson, 2008). To gain a clearer picture of the prevalence of each of the three types of attacks and to obtain a better understanding of the composition of typical hacking attacks, all three types of attacks were assessed independently.

Table 5: Measurements of Hacking Activity – Technical Intrusions

Variable	N[1]	%[2]
Total number of technical intrusions		
Up to 5	27	21.8
6-10	16	12.9
11-50	20	16.1
51-100	11	8.9
101-500	25	20.2
501-20,000	25	20.2
Frequency of technical intrusions (per year)		
1	26	21.0
2-6	30	24.2
7-12	12	9.7
13-36	17	13.7
37-156	22	17.7
157-2,500	17	13.7
Success rate in % (st. dev.)	124	48.1 (2.5)

[1] The total sample size is n=124.
[2] Percentages may not add up due to rounding.

Table 5 shows a bimodal distribution for the number of technical intrusions. Most hackers were either very engaged or hardly active at all. The four most active hackers in

the sample each reported to have committed an estimated total of 20,000 hacking attacks over the course of their careers. A total of 20 percent of all respondents in the sample indicated having hacked between 500 and 20,000 times and another 20 percent said they had hacked between 100 and 500 times. The results in Table 5 clearly show that the convention was attended by many veteran hackers.

The frequency measure of technical intrusions per year further confirmed that many of the interviewed hackers were regularly hacking at the time the survey was conducted. A total of 30 percent of all respondents reported having attempted from three hacks per month to an astonishing seven hacks per day. Obviously, a number of seven hacking attempts per day can only be achieved when the single hacking attempts are committed through highly automated attack routines and without any sophisticated preparation routines. An investigation into the cases with extremely high frequencies and numbers of total hacks revealed that they did indeed report very short preparation times and many of them also reported low to moderate success rates. Overall, the success rate reported by all respondents showed that they considered about half (48 percent) of all technical intrusions to have been successful.

A 50 percent success rate of all technical intrusions was already very high, but, as Table 6 shows, the success rate of social methods was even higher (62 percent). The very high success rate of social methods was one of the most surprising findings in this study. It demonstrates that the popular image of hackers as social hermits who launch their hacking attacks solely through remote computer and network technology, or even do so mainly to compensate for social deficits, has to be revised. The opposite

seems to be the case. Hackers seem to be very socially intelligent persons who know how to successfully manipulate and trick other persons.

Table 6: Measurements of Hacking Activity – Social Methods

Variable	N[1]	%[2]
Types of social methods		
Social engineering	94	75.8
Shoulder surfing	81	65.3
Dumpster diving	51	41.1
Impersonation	46	37.1
Deception	36	29.0
Bribery	18	14.5
Total number of social methods		
0	17	13.7
1-5	24	19.4
6-10	20	16.1
11-50	14	11.3
51-100	11	8.9
101-500	21	16.9
501-5,000	17	13.7
Frequency of social methods (per year)		
0	18	14.5
1	31	25.0
2-6	23	18.5
7-12	7	5.6
13-36	9	7.3
37-156	25	20.2
157-365	11	8.9
Success rate in % (st. dev.)	107	71.8(2.4)

[1] The total sample size is n=124.
[2] Percentages may not add up due to rounding.

More detailed case examinations of the hackers who reported the highest success rates with their social hacks revealed that they were the same hackers who also reported to have the most success with their technical intrusions. Moreover, most of these very successful hackers gave almost identical numbers and frequencies for the

two methods. Based on these observations, one can conclude that the most successful hackers are the ones who combine social and technical approaches in their hacks.

All six of the listed social attack methods shown in Table 6 were used by an unexpectedly high number of hackers. The most popular type of the social attack methods was social engineering. Three-fourth of all respondents reported to have used social engineering methods in their hacks. Surprisingly, shoulder surfing was the second-most, and dumpster diving the third-most popular method. The large popularity of these two simple methods (65 and 41 percent) shows that hacking attacks do not always have to be sophisticated attacks and require a lot of knowledge, preparation, and expertise. They can be as simple as watching other computer users type in their login passwords or searching their garbage for sensitive information that can then be exploited. The two more sophisticated social methods, impersonation and deception, were used by fewer hackers than the more simple methods, but they were still considerably popular. Thirty-seven percent of all respondents reported to have used impersonations, and 29 percent indicated that they have engaged in deceptions to trick persons for hacking purposes. Bribery was the least common technique of all social methods. Still, a total of 15 percent of all respondents had employed this method for their hacks.

The unexpected popularity of social methods was corroborated by the two items measuring the total number of social hacks and the frequency with which they were employed. Even though the highest total number of social hacks was considerably lower than that for technical intrusions, 30 percent of all respondents still reported to have conducted more than 100 such attacks over the course of their careers. Only 14 percent of all participants said that they had never engaged in any such methods. Another sur-

prising finding was that, even though the highest frequency with which social methods were applied (1 per day) was again lower than the highest frequency of technical intrusions (7 per day), the percentage of hackers who reported to engage in three social attacks per month or more was roughly the same as for technical intrusions (29 versus 30 percent).

Table 7: Measurements of Hacking Activity – Malware Distribution

Variable	N[1]	%[2]
Types of distributed malware		
Trojan Horses	20	16.1
Adware/Spyware	0	
Viruses/Worms	11	8.9
Spam/Phishing mails	9	7.3
Other	15	12.1
None	87	70.2
Total number of distributed malware		
0	87	70.2
1-5	22	19.4
6-10	4	3.2
11-50	2	1.6
51-100	5	4.0
101-1,000	4	3.2
Frequency of distributed malware (per year)		
0	87	70.2
1	24	18.5
2-6	3	2.4
7-12	8	6.4
13-36	0	
37-200	2	1.6
Success rate scale 1-7 (std. dev.)	37	$\bar{x}$=3.6 (0.9)

[1] The total sample size is n=124.
[2] Percentages may not add up due to rounding.

In addition to technical intrusions and social methods, the survey also asked respondents about types of malicious code that they had ever distributed. Table 7 shows the descriptive statistics for the distribution of malicious code. Different from the large popularity of the first two methods, distributions of malicious code were relatively uncommon, and the type of malicious codes that had been distributed was highly diversified. Seventy percent of all hackers in the sample reported never having distributed any type of malicious codes. The types of malware that were most often used were Trojan horses (16 percent) and viruses (11 percent). The 15 persons who marked “Other” forms of malware most often specified that they designed their own scripts and were circulating custom-made program codes or other forms of highly specialized code such as SQL injections.

A noteworthy finding was the unpopularity of spam or phishing emails (7 percent) and adware or spyware (0 percent). The results in Table 7 suggest that hackers and phishers or spammers are two separate types of cyber-criminals. This conjecture was reaffirmed by additional case analyses of active distributors of malware. The respondents who most often circulated malicious code rarely engaged in technical or social hacking methods. Thus, while classic hackers oftentimes combined technical intrusions and social engineering methods, or at least engaged frequently in both of them, they were distinctively different from the persons who circulated the most malicious code. The latter appeared to have a hacking profile that is distinctively different from the former two.

Since the success rate of malware distributions is not simply determined by any definite success versus failure ratio but by the total numbers of infected computers, the

success rate of malware distributions was measured on a seven-point Likert type scale. The results of this measure suggest that hackers who distributed malware were estimated to have a medium level of success with their efforts ($\bar{x}$=3.6).

The Developments During the Habituation of Hacking

The lengths of hacking careers in Table 8 reaffirmed the considerable experience of most hackers in the present sample. The normal-shaped distribution of hacking experiences ranged from less than a year to 28 years and averaged at ten years. The length of most hacking careers in the present sample was a clear indication that the majority of respondents were not beginners, but had already habitualized their hacking activities.

As was predicted by the rational choice perspective, most respondents befriended other hackers during their time as active hackers. Seventy-five percent of all respondents said they had changed their social networks to include other hackers, and 23 percent did so “very much.” Alongside the changes in their networks, most hackers also reported changes in their motives, their engagement in hacking, and their skills. Only one respondent said that he had not improved his hacking skills since he began hacking. As expected, this particular hacker was one of the least experienced in the sample. He had less than one year of hacking experience and had committed only one single hack. All other respondents claimed to have improved their skills over the course of their careers, and 72 percent said they did so “very much.”

Table 8: Developments during Hacking Career

Variable	N[1]		% [2]	
Time hacking (in years)				
Up to 1	8		6.5	
2-5	30		24.2	
6-10	47		37.9	
10-15	20		16.1	
16-20	10		8.1	
20-28	9		7.3	
Change friends (more hackers)				
Yes, very much	28		22.6	
Yes, somewhat	66		53.2	
No	30		24.2	
Improved skills				
Yes, very much	89		71.8	
Yes, somewhat	34		27.4	
No	1		0.8	
Hacking more frequent				
Yes, very much	37		29.8	
Yes, somewhat	39		31.5	
No, it's the same	18		14.5	
No, it's less frequent	30		24.2	
Motives changed				
Yes, very much	38		30.6	
Yes, somewhat	37		29.8	
No	49		39.5	
Current primary motive (initial interest)				
Intellectual curiosity	37	(74)	29.8	(59.7)
Financial gain	28	(0)	22.6	
Experimentation	22	(21)	17.7	(16.9)
Other	21	(4)	16.9	(3.2)
Excitement, thrill, fun	14	(15)	11.3	(12.1)
Self-concept boost	2	(2)	1.6	(1.6)
Feeling of power	0	(4)		(3.2)
Political ideology	0	(2)		(1.6)
Peer recognition	0	(1)		(0.8)
Personal revenge	0	(1)		(0.8)

[1] The total sample size is n=124.
[2] Percentages may not add up due to rounding.

A majority of respondents reported that their hacking activities had intensified over the course of their careers. Of all hackers in the sample, 30 percent said they are hacking much more frequently now than when they started, and 32 percent reported that their hacking activities have somewhat increased. Only 30 respondents (24 percent) said their hacking activities had become less frequent. Of those, 27 also said that they are no longer actively hacking. Thus, only 3 active hackers had decreased their hacking frequency and 60 percent of the still active hackers had increased it. The data shows an apparent trend toward an intensification of hacking activities over time.

Sixty percent of respondents further indicated that their motives had changed since their initial interest in hacking. Indeed, the comparison of initial motives with current ones revealed three dramatic changes that had occurred between the two measures. First, the importance of intellectual curiosity as the primary motive had decreased by 50 percent over time (from 60 to 30 percent). Second, financial gain, a motive of no importance for the initial interest, had become the second-most important motive for hacking. Twenty-three percent of all subjects said that their main motives for continuing to hack were financial gains. The sharp increase of financial gains as motives for hacking is an intriguing finding. It means that, while most hackers set out to become hackers because they are curious about the technology and keen to experiment with it, along the way some of them realize the financial possibilities that are achievable through their engagement in hacking. The third main difference between the two measures is the reduction of motives. While the list of initial motives included ten different motives, this list was reduced to only six persistent motives. Feelings of power, political ideology, peer recognition, and personal revenge no longer played a role for the continued engage-

ment in hacking. The changes in motives demonstrate that for many, hacking efforts evolved into a professional business. This trend was also reflected in the “Other” category. Most entries in this category pertained to the gathering of sensitive and security-related information.

The changes in motives were mirrored in the changes that occurred in the preferences for certain targets. As Table 9 illustrates, 71 percent of all respondents reported to have changed their targets over the course of their careers. Also, 50 percent said they are now attacking higher profile targets and 86 percent reported to have changed their methods and tools to attack the different kinds of targets.

The increased preference of many hackers for higher profile targets was visibly reflected in their preferred types of targets. Both corporate and governmental targets were attacked much more frequently. The preference for corporate computers quadrupled (from 4 to 17 percent), the preference for corporate networks septupled (from 6 to 40 percent), and the preference for corporate websites increased twelvefold (from 2.4 to 28 percent). Similarly, governmental targets, which were virtually not targeted during the onset of the hacking activity, were much more popular among experienced hackers. Fifteen percent reported having attacked governmental hosts, 25 percent attacked governmental networks, and 20 percent targeted governmental websites.

Table 9: Target Preferences

Variable	N[1]	% [2]
Targets changed since 1st hack		
Yes, very much	52	41.9
Yes, somewhat	36	29.0
No	36	29.0
Higher profile targets		
Yes, very much	29	23.4
Yes, somewhat	34	27.4
No	61	49.2
Current target owner / type	N (%)[3]	N (%)[3]	N (%)[3]
	Single host	Network	Website
Private	49 (39.5)	56 (45.2)	23 (18.5)
Corporate	21 (16.9)	49 (39.5)	35 (28.2)
Non-profit	4 (3.2)	4 (3.2)	7 (5.6)
Government	18 (14.5)	31 (25.0)	25 (20.2)
Current target selection criteria (initial criteria)		
Easy access	58 (70)	46.8 (56.5)
Interesting information	87 (36)	70.2 (29.0)
Profitable information	31 (0)	25.0
Reputation gain	2 (0)	1.6
Antipathy	2 (7)	1.6 (5.6)
Other	11 (11)	8.9 (8.9)
Rejection reasons		
No interesting information	60	48.4
Unfamiliarity with architecture	48	38.7
Sympathy with host	23	18.5
No profitable information	19	15.3
Other	9	7.3
None of the above	30	24.2
Change in methods and tactics		
Yes, very much	51	50.0
Yes, somewhat	37	36.3
No	14	13.7
Variability of methods (scale 1-7)	123	4.7 (1.7)
Variability of tools (scale 1-7)	123	3.9 (1.7)

[1] The total sample size is n=124.
[2] Percentages may not add up due to rounding.
[3] Multiple answers were possible. % values refer to complete sample.

The selection criteria for targets changed in accordance with the motives and the targets. The prospect of obtaining profitable information, initially irrelevant during the onset of hacking activities, had become the third-most important criterion. Twenty-five percent of all respondents said this criterion was relevant for their selection of targets. The significantly increased importance of profitable information further confirmed the trend toward a professionalization of illegal activities. Easy access remained the most important criterion, but its significance was notably reduced (from 57 to 47 percent). Following an opposite trend, the prospect of interesting information had vastly gained importance. More than double as many hackers listed interesting information as one of their selection criteria (from 29 to 70 percent).

Among rejection criteria, the absence of interesting information was the most frequent one. Almost half of all participants (48 percent) listed it as a reason to refrain from an attack. Unfamiliarity with the architecture of a computer system or network was the second-most common reason for a rejection (39 percent), followed by sympathy with the host of that system or network (19 percent). Analogous to its importance as a selection criterion, 15 percent of all hackers in the sample marked the absence of profitable information as a reason for rejecting a particular target. This result underlines the profound change many hackers undergo over the course of their hacking careers. Hackers apparently become more professional and many of them begin to see hacking not only as an intellectual challenge, but as a potential source of income.

Table 10 illustrates that the question asking respondents whether hacking for them is a source of income was positively confirmed by 41 percent. Fifteen percent even identified hacking as their main source of income. An additional case analysis

found that these 15 percent were mostly the same hackers that also reported to reject a target if it has no profitable information to offer.

The Risk-Avoidance Efforts and Desistance Considerations

The last section of hacking-activity related questions in the survey asked respondents about their efforts to minimize risks, their risk estimates, and their readiness to desist from hacking. The results of these items are displayed in Tables 10 and 11. The results in Table 10 confirm the appropriateness of the anonymizing tactics that were provided as answer categories. Only 5 percent said they used methods other than the ones provided for this item. In contrast, the least popular method on the list (source routing) was used by 15 percent of the respondents in the sample. More than 50 percent of all participants used the three most common methods. Proxies (60 percent), war driving (57 percent), and spoofing (54 percent) all share in common that they are relatively simple and effortless methods. As Table 10 shows, an inverse correlation seemed to exist between the technical difficulty of anonymizing methods and their popularity. The explanation for this inverse correlation is simple. The multitude of relatively simple methods that already grant a high degree of anonymity in cyberspace made using more strenuous tactics unnecessary.

When asked whether they had ever considered desisting from hacking, a total of 45 percent of all respondents answered “yes.” However, only six hackers (5 percent) said they had done so often. An examination of these six cases showed that all of them also reported to no longer be actively hacking. Unfortunately, the small case number in the present sample renders this dataset unsuitable for further investigations of signifi-

cant differences between those cases and the ones that had not considered quitting or those who considered quitting a few times.

Table 10: Anonymizing Methods and Desistance Considerations

Variable	N[1]	%[2]
Anonymizing methods[3]		
Proxies	74	59.7
War driving	71	57.3
Spoofing	67	54.0
Public access points	55	44.4
Tunnels, Covert channels	54	43.5
TOR, I2P, etc.	49	39.5
Bouncing	33	26.6
Source routing	19	15.3
Other	6	4.8
Hacking source of income		
Yes, the main	18	14.5
Yes, but not the main	33	26.6
No	73	58.9
Considering quitting		
Yes, often	6	4.8
Yes, a few times	50	40.3
Never	68	54.8
Reason for considering quitting[3]		
Involved risk	27	21.8
Fear of prosecution	21	16.9
Fear of apprehension	15	12.1
Involved effort	11	8.9
Fear of detection	9	7.3
Other	8	6.5
Income too irregular	6	4.8
Legal alternatives	5	4.0

[1] The total sample size is n=124.
[2] Percentages may not add up due to rounding.
[3] For better readability, categories are rank ordered by importance.

The hackers who had considered quitting reported to have done so mainly because they were worried about the involved risk in general (22 percent). Seventeen percent considered quitting because they were afraid of being prosecuted, 12 percent did so because they were afraid of being apprehended, and 7 percent thought about quitting because they were afraid of being detected. The lesser importance of the fear of detection and apprehension might be initially counter intuitive, given that a prosecution implies a prior detection and apprehension. However, the greater fear of prosecution simply illustrates the fact that the prospect of being prosecuted is a greater deterrent than the prospects of being detected or apprehended.

Compared to the fears of getting caught, a relatively small number of hackers (18 percent) also reported having considered quitting because of various practical reasons. For 9 percent, the involved effort was a reason to contemplate giving up hacking. Another 5 percent said that the income yielded by hacking was just too irregular, and 4 percent considered switching to legal alternatives.

Table 11 shows that, when asked whether they were more or less afraid of being tracked and apprehended now than when they started to hack, slightly more than one-third of all respondents reported to be more afraid today (37 percent). Thirty-four percent said their level of being afraid had not changed, and another 30 percent said they were less afraid today (15 percent) or had never been afraid (15 percent). The slightly higher percentage of hackers who report to be more afraid today suggests that the increased efforts of law enforcement agencies in combating cyber-criminals has not gone unrecognized in the hacking community. However, they also indicate that many hackers are well aware of the continuing slim chances of becoming tracked and apprehended.

Many hackers further rated the risk of becoming apprehended significantly lower than that of being detected. Thus, they demonstrated awareness of the fact that, due to the various difficulties involved in the prosecution of cybercrimes, detection does not necessarily imply apprehension. Nevertheless, the popularity of the various anonymizing methods and the high fraction of aborted hacking attacks (about 20 percent) were clear indicators of the efforts many hackers undergo to avoid detection.

Table 11: Risk Estimates and Carefulness

Variable	N[1]	%[2] (sd)
Afraid of being tracked and apprehended		
More afraid	46	37.1
Unchanged	42	33.9
Less afraid	18	14.5
I was never afraid	18	14.5
Preparation and planning time		
Less than 2 hrs	10	8.1
2 hrs	20	16.1
3 hrs – 1 day	30	24.2
2 days	24	19.4
3 – 5 days	24	19.4
2 – 3 weeks	13	10.5
Over 3 weeks	3	2.4
Change in preparation time		
More time today	63	50.8
About the same time	44	35.5
Less time today	17	13.7
Risk of detection estimate (scale 1-7)	124	3.6 (1.1)
Risk of apprehension estimate (scale 1-7)	124	2.5 (1.4)
Focus on rewards (1) vs. risks (7)	124	3.7 (1.2)
Rational (1) vs. emotional (7) during hacks	124	2.4 (1.4)
% of aborted attacks	124	20.4 (2.0)

[1] The total sample size is n=124.
[2] Percentages may not add up due to rounding.

In concordance with the changes found in motives, targets, and methods, the increasing professionalism of many hackers was also manifested in their more careful preparations. About half of all respondents reported to invest more time in their preparations today than when they started, a significantly higher number than the 14 percent who prepare less today. On average, hackers dedicated between three to eight hours to preparing their hacks. The length of preparation distribution, however, shows great variability and ranges from less than two hours to several weeks in some extreme cases.

The Assessment of Scale Validity and Reliability

The regression models used for the testing of the research hypotheses operated with two of the personality constructs (risk propensity and rationality) as independent variables. To ensure the appropriate operationalization of all personality variables in the regression models, the validity and reliability of the personality constructs was assessed prior to the calculation of the regression models. When estimating the validity of a theoretical construct, two aspects are of particular importance: discriminant and convergent validity (Schnell, Hill, & Esser, 1999; Trochim, 2002). Discriminant validity is achieved when a construct is empirically distinguishable from other constructs (Straub, 1989), and convergent validity is confirmed when all items comprising the construct are measuring only aspects of the intended construct. At the same time, a construct also has to be reliable, i.e. internally consistent. Internal consistency is achieved when all items comprising the construct are highly inter-correlated. Since the scales used to measure the personality constructs were abbreviated and partially modified, the validity and reliability of these scales was analyzed in an exploratory validation phase.

The Exploratory Factor Analysis

According to Thompson (2004), an exploratory factor analysis (EFA) should be conducted when the relationships between individual items and underlying factors are not exactly known. Since the risk propensity scale consisted of items from different scales and the Rational-Experiential Inventory scale was heavily abbreviated, EFA was used for a confirmation of the convergent and discriminant validity of the measures. The particular type of EFA was a principal component analysis with promax rotation and Kaiser normalization (calculated with SPSS 16.0). As Hair and his colleagues suggested, the selection of an orthogonal or oblique rotation should be made according to the specific demands of a particular research problem (Hair, Anderson, Tatham, & Black, 1998). According to Hair et al., orthogonal rotation methods are most appropriate when the research goal is to reduce the number of items in a construct, regardless of how meaningful the resulting underlying factors are. On the other hand, if the intent is to create or verify theoretically meaningful constructs, oblique rotation methods are better suited. Since the purpose of this factor analysis was to reveal the appropriateness of the scales used in this study, promax rotation, an oblique rotation method, was chosen over orthogonal rotation. All 15 items were entered into the EFA and three factors were extracted. Table 12 presents the EFA results for all three personality variables.

Table 12: Personality Scales, Item, Factor, and Index Analysis

Items	Item to total correlation	Factors[1] 1	2	3
Risk propensity scale (α=.83)				
I always try to avoid situations involving a risk of getting into trouble.	.65	.81		
I always play it safe even when it means occasionally losing out on a good opportunity.	.69	.88		
I am a cautious person who generally avoids risks.	.71	.83		
I am rather bold and fearless in my actions.[2]	.52	.63		
I am generally cautious when trying something new.	.53	.65		
Rationality items (α=.75)				
I usually have clear, explainable reasons for my decisions.	.62		.79	
I don't reason well under pressure.[2]	.55		.81	
Thinking hard and for a long time about something gives me little satisfaction.[2]	.44		.57	
I prefer complex to simple problems.	.42		.57	
I enjoy solving problems that require hard thinking.	.63		.82	
Intuition-experience items (α=.86)				
Using my gut-feelings usually works well for me in working out problems in my life.	.57			.73
I trust my initial feelings about situations.	.66			.82
I like to rely on my intuitive impressions.	.79			.87
I often go by my instincts when deciding on a course of action.	.79			.86
I don't think it is a good idea to rely on one's intuition for important decisions.[2]	.61			.86
Eigenvalue		2.71	2.21	4.31
Variance explained (%)		18.1	14.8	28.7
Cumulative variance (%)		18.1	32.9	61.6

Indices	α	N	Range	$\bar{x}$	(sd)
Summative risk propensity index	.83	124	5-35	22.1	6.1
Summative rationality index	.75	124	11-35	27.2	5.0
Summative intuition index	.86	124	10-35	23.6	5.3

[1] Principal Component Analysis with Promax Rotation Method and Kaiser Normalization. Loadings less than .4 not shown.
[2] Items were reversed.

Table 12 shows that the EFA produced three factors with eigenvalues greater than 2.0, a level that confirms the independence of the concepts. The high eigenvalues of all three factors also indicated that the factors explained large fractions of the variance within their respective set of variables. The three factor solution accounted for 63.4 percent of the total variance, a value above the generally accepted 60 percent level in social research (Hair et al., 1998; Thompson, 2004). To assess the factor loadings in the individual item analysis, guidelines from Kim and Mueller (1978) were used. According to these guidelines, loadings of 0.4 to 0.54 are considered fair; 0.55 to 0.62 are considered good; 0.63 to 0.70 are considered very good; and over 0.71 are considered excellent.

As Table 12 shows, all of the 15 items loaded higher than 0.55 on their respective factors, and none of the items loaded higher than 0.4 on any other factors. Thus, all three constructs were extracted “cleanly” as factors. The fact that none of the items loaded on multiple factors was a strong sign that all three personality constructs had high levels of discriminant validity. Similarly, the high to excellent loadings of all individual items on their respective factors further suggested that all three constructs also had high levels of convergent validity. Based on the positive EFA results, all of the 15 items were retained in the analysis

All 15 items also correlated highly with their respective scales. The lowest item to total correlation of any item was 0.42, which shows that all items contributed in a meaningful way to the scale scores. The high internal consistency of all three scales is further reflected in their high Cronbach’s alpha values. The risk propensity scale reached an alpha level of 0.83, the rationality scale a level of 0.75, and the experience scale a

level of 0.86. All three values were within 0.70 and 0.90, the range that is typically considered to be ideal for internal consistency measures (Hair et al., 1998).

Overall, the loading patterns of the REI items in this factor analysis compared favorably to the factor analysis findings for the complete scales that were reported by Handley and colleagues (Handley et al., 2000). The similarity between the patterns of both factor analyses confirms the appropriateness of the item selections that were used to create the abbreviated scales. The comparison to Handley's results further reveals an interesting finding. When compared to the general public sampled in Handley's study, the sample of hackers yielded a considerably higher average rationality value (5.4 compared to 3.4 in Handley's analysis). Hackers also reported to have a higher confidence in their experience-based decision making (4.7 compared to 3.4), even though this difference was not as large as the one found between the two rationality measures. These comparisons suggest two important differences between hackers and the general public: (1) hackers prefer a more analytical and rational thinking style than the average person, and they (2) display a generally higher confidence in their ability to make decisions, regardless of whether these decisions are based on rational considerations or on intuition and experience.

The Test of the Study Hypotheses

All of the hypotheses tested in this study were assessed using additive multivariate linear regression models. The personality scales were recoded into summative indices and included as independent variables in the regression models. For the creation of the indices, all negative items were reversed so that higher values in all variables re-

flected more pronounced personality characteristics. The calculation of the summative indices was unproblematic because none of the scale items had any missing values and none of the indices contained any extreme outliers. Table 12 provides detailed statistical descriptions of all three indices.

In addition to the two variables testing the predictions derived from RCP, seven main sociodemographic variables were included in the saturated models to control for potential effects of external factors. The seven variables included in the analysis were age, gender, race, educational attainment, employment status and student status. The age variable was calculated by subtracting the respondents' year of birth from 2008, and included as a continuous variable. Given that the conference took place in February, this calculation method yielded the correct age of most participants. Sex (1 indicating females), race (1 indicating Non-Whites), marital status (reference category never been married), employment status (1 indicating unemployed), and student status (1 indicating students) were coded as indicator variables. The decision to collapse some of the subcategories in these variables was made in order to avoid problems that might result from the low cell counts of some of these variables. Black, Asian, Hispanic, and Other respondents, which together had a cell count of 11 cases, were collapsed into one single category Non-Whites. The reference category "never been married" was chosen for marital status because most respondents fell in this group. The one respondent who reported to be divorced was included in the next closest category "married." The variable measuring educational attainment was included in the models in its original coding. The inclusion of ordinal scaled variables in linear regression models, even though debated by some researchers since the early 1970s (Hawkes, 1971; Morris,

1970), has become a common practice and has repeatedly been proven to produce viable results (Allan, 1976; Kim, 1978; O'Brian, 1979).

Before the regression models were run, the conformity of the present data with several assumptions of these models was verified to avoid any potential violations. First, all variables were screened for outliers. Given the small number of cases in some of the subgroups (7 females, 11 Non-Whites, 10 unemployed), this step was particularly important. As a result of this screening process, three cases were excluded from the third regression analysis because their values on the dependent variable were four to ten times higher than the next highest values. If included in the regression model, these cases would have exerted a disproportional influence on the results. Next, all variables were screened for multicollinearity. With the tolerance levels of all independent variables over 0.9, no linear inter-correlation was detected among them. The results of the various regression models are displayed in Tables 13, 14, 15, and 16.

The Test of Hypotheses H1 and H2

Table 13 shows the influence of the two personality characteristics, risk propensity and rationality, on the overall success of hacking activities. To reflect the overall success of all hacking activities most accurately, the success rates of the three different attack methods (technical intrusions, social methods, and malicious code distributions) were weighed with the proportion of total hacking attempts that was accounted for by the respective attack method, and all three products were then summarized into the total success rate for all methods. For example, if a hacker reported having undertaken a total of 100 hacking attempts, out of which 70 were technical intrusions, 20 were social

engineering attacks, and 10 were distributions of malicious code, the total success rate for this hacker was calculated as the sum of the success rate of technical intrusions multiplied by 0.7, the success rate of social methods multiplied by 0.2, and the success rate of malicious code distributions multiplied by 0.1.

The regression results presented in Table 13 clearly support the predictions that were derived from the propositions of the rational choice perspective. Despite the low number of cases in the models (n=124), a circumstance that usually causes high in-group variances, both models were highly significant (Model 1 and 2 $p<.001$).

Table 13: OLS Regression Coefficients for Estimated Effects of Rationality and Risk Propensity on Hacking Success

	Model 1		Model 2	
Variable	B	β	B	β
Hypothesized characteristics				
Rationality index	.14 **	.29 (.04)	.14 **	.30 (.04)
Risk propensity index	-.09 **	-.23 (.04)	-.09 *	-.23 (.04)
Sociodemographic controls				
Age			.00	.00 (.04)
Female			.13	.01 (.97)
Non-White			-1.66 *	-.19 (.77)
Education			-.12	-.06 (.22)
Marital status				
Living as married			-.41	-.06 (.64)
Married			.20	.04 (.57)
Unemployed			-1.30	-.15 (.97)
Student			-1.03 *	-.20 (.97)
Constant	4.09 **	(1.27)	5.03 **	(2.00)
R-squared	.11		.21	

*$p<.05$. **$p<.01$. ***$p<.001$

In the first model, the two personality characteristics alone explained 11 percent of the variance in the success of hacking attacks. In this model, both variables exerted a highly significant influence on the dependent variable ($p<.01$). Moreover, rationality turned out to be the most influential variable in both models. As was predicted in the hypotheses, the effect of rationality on the success of hacking attacks was positive and the effect of risk propensity negative. The results confirm the predictions made in hypotheses H1 and H2 in Chapter 5: The higher the preference for an analytic-rational approach to thinking and the lower the risk propensity of a hacker, the more successful this hacker is in his or her hacking activities.

The inclusion of the sociodemographic control variables in the second, saturated model had only a slight impact on the effect of both personality variables. While the standardized coefficients for both variables remained roughly the same, the inclusion of the control variables reduced the effect of risk propensity to a $p<.05$ significance level. Overall, the inclusion of the additional variables raised the amount of explained variance to 21 percent in the second model. Nevertheless, the impact of the individual sociodemographic variables was surprisingly small. Only two of the variables reached a significant level. The variables age and sex had virtually no impact on the dependent variable. Particularly for the age variable, this finding was surprising because it implies that, despite the fact that virtually all hackers in the sample reported to have increased their hacking skills over the course of their hacking careers, hackers of all ages report roughly the same success rates. One possible explanation for this finding is that more seasoned hackers also report to seek out higher profile targets and that this change in tar-

get preference countervails the improvements of hacking skills. This explanation, however, remains speculative and requires further testing to be confirmed.

Different from the surprising finding with regard to age, the complete absence of a gender effect in the data is unfortunately not very meaningful because only seven of the respondents were females. Since seven respondents are not enough cases to allow a confident generalization of the results, future studies with more female hackers are needed to confirm this finding. The only two sociodemographic variables in the second model to reach a significant level were race and student status. Students report significantly lower success rates than persons who are not or no longer studying. Also, when compared to White hackers, hackers belonging to minority groups report a significantly lower success rate (I<.05). However, this finding also has to be interpreted with caution, given the small number of minority hackers in the present sample.

The Test of Hypotheses H3 and H4

The predictions of hypotheses H3 and H4—that hackers with a higher preference for analytic-rational thinking and a lower risk propensity will also perceive their hacking activity as riskier—were tested with a second regression analysis. For the assessment of the overall risk estimation in the dependent variable, the two items measuring the estimated risks of (1) being detected and (2) being apprehended during or after a hack were combined into one summative index. As did the other indices, this index had no missing values and showed no significant deviation from a normal distribution.

Table 14: OLS Regression Coefficients for Estimated Effects of Rationality and Risk Propensity on Perceived Risk Involved in Hacking

Variable	Model 1 B	Model 1 β	Model 2 B	Model 2 β
Hypothesized characteristics				
Rationality index	.11 **	.25 (.04)	.13 ***	.30 (.04)
Risk propensity index	-.10 **	-.27 (.03)	-.11 ***	-.30 (.03)
Sociodemographic controls				
Age			-.11 **	-.32 (.04)
Female			1.67 *	.17 (.86)
Non-White			-1.99 **	-.25 (.67)
Education			-.09	-.05 (.19)
Marital status				
Living as married			.16	.02 (.57)
Married			.22	.05 (.50)
Unemployed			-1.27	-.16 (.86)
Student			-1.43 ***	-.30 (.44)
Constant	5.32 ***	(1.17)	9.37 ***	(1.76)
R-squared	.11		.29	

*p<.05. **p<.01. ***p<.001

The results of the regression models corroborated the predictions stated in the theoretical hypotheses. Both models were highly significant (Model 1 and 2 p<.001), and the two personality characteristics exerted highly significant effects on the dependent variable in Model 1 (p<.01) and Model 2 (p<.001). Thus, hackers with a preference for an analytic-rational thinking style estimate the risks involved in their hacking activities to be significantly higher, as do hackers with a lower risk propensity. While this result is little surprising for the risk propensity variable, the finding that the standard coefficient of the rationality variable is almost as high as that of the risk propensity variable implies that hackers with higher rationality scores weigh the potentially involved risks considerably more in their decision-making processes. In combination with the results of

the first regression analysis, this finding suggests that it is the most successful hackers who are also most susceptible to changes in the estimated risks. Together, these two findings hold important policy implications because they indicate that successful manipulations of risk estimations might be a suited tactic to deter especially higher skilled hackers.

The circumstance that the significance level of both personality characteristics increased with the inclusion of the control variables in the saturated model hints at a slight suppression effect. The one sociodemographic variable that was identified to exert this suppression effect was student status, a variable that had a highly significant effect itself ($p<.001$). Aside from the student status variable, age ($p<.01$), gender ($p<.05$), and race ($p<.01$) also exerted a significant effect on the risk perception. The findings that student hackers have significantly lower risk estimates, whereas female hackers estimate risks to be significantly higher are consistent with many other studies in the literature (Bouffard, 2007; Earnest, 2003; Paternoster, 1989; Wright, Caspi, Moffit, & Paternoster, 2004). Contrariwise, the findings that older hackers have lower risk perceptions, while minority hackers have higher ones, appear to be counterintuitive at first. The effect measured with regard to age, however, is consistent with the predictions of RCP. Rational choice perspective assumes that the awareness of involved risks decreases during the habituation of the activity. During this phase, the criminal activity becomes a routine exercise and the absence of any negative consequences diminishes the awareness of involved risks over the years.

The finding that minority hackers report higher risk estimates, while interesting, has to be interpreted with caution because the number of minority hackers included in

the sample was too small to allow meaningful generalizations. Future studies with larger samples of minority hackers are again required to confirm this finding.

The Test of Hypotheses H5 and H6

As was mentioned earlier, three cases were excluded from the third regression analysis due to their extreme values on the dependent variable. The third analysis regressed the time that hackers reported to use for the preparation of their attacks on personality traits and sociodemographic characteristics. Three of the respondents reported preparation times that were four to ten times longer than the next longest time intervals. Two of the cases reported to prepare their attacks for three months, and one respondent indicated it takes him a whole year to prepare a single hack. An examination of the three cases revealed that all three cases engaged in hardly any hacking activity and probably counted the time intervals between hacks as preparation time. Based on the results of this examination, all three cases were excluded. After the exclusion of the three outliers, the dependent variable was no longer significantly skewed. The results of the third regression analysis are shown in Table 15.

The results shown in Table 15 corroborate hypothesis H5, but they lend only partial support to hypothesis H6. As was the case in the other regression analyses, both models in the third regression analysis were significant ($p<.01$). The rationality variable was again the strongest predictor variable in both models ($p<.01$ in Model 1 and $p<.05$ in Model 2). The effect of the risk propensity variable pointed in the predicted direction in both models, but the effect reached a significant level only in the second, saturated model ($p<.05$). Again, the student variable was identified as responsible for the slight

suppression effect (Cramer, 2003). Despite the fact that none of the sociodemographic variables reached a significant level, the proportion of explained variance in the dependent variable increased from 11 percent in the first model to 21 percent in the second model.

Table 15: OLS Regression Coefficients for estimated Effects of Rationality and Risk Propensity on Preparation Time

	Model 1[1]		Model 2[1]	
Variable	B	β	B	β
Hypothesized characteristics				
Rationality index	1.3 **	.25 (.50)	1.2 *	.22 (.53)
Risk propensity index	-.76	-.17 (.41)	-.87 *	-.20 (.44)
Sociodemographic controls				
Age			.20	.05 (.51)
Female			-1.40	-.11(13.0)
Non-White			-1.57	-.16 (9.1)
Education			1.97	.09 (2.6)
Marital status				
Living as married			-3.04	-.04 (7.6)
Married			-6.40	-.11 (7.0)
Unemployed			6.18	.06(11.7)
Student			1.12	.02 (5.9)
Constant	2.61	(14.6)	-4.54	(23.8)
R-squared	.11		.21	

*p<.05. **p<.01. ***p<.001
[1] n=121. 3 outliers were excluded.

The analysis demonstrates that hackers with a higher preference for a rational thinking style prepare for their hacking attacks longer. The longer time period used for preparation is an indication for an overall more thorough preparation process. The longer preparation phase reduces the involved risks and it probably also contributes to the

overall higher success rate of more rational-acting hackers and hackers with a lower risk propensity.

The Test of Hypotheses H7

The last hypotheses H7 stated that risk propensity also exerts an influence on the total number of hacking attempts. The dependent variable total number of hacking attempts was calculated as a summative index of the total number of technical intrusions, social methods, and malware distributions a person had attempted. The wide range of the index (it ranged from 1 to 23,000) and the rounded estimates many respondents gave to the questions about the total number of attacks caused the dependent variable to have a platykurtic shape with a multimodal, rounded peak and wide shoulders. Despite the significant deviation from the mesokurtic shape of a normal distribution, the distribution of the dependent variable was not significantly skewed, and was therefore included in the regression.

Different from the other three regression analyses, the effect of the risk propensity variable ($p<.001$ in both models) was stronger in this analysis than the effect of the rationality variable. Nevertheless, an unpredicted significant effect was also found for the rationality variable ($p<.05$ in Model 1 and $p<.01$ in Model 2). The effects of both variables are shown in Table 16.

The risk propensity of respondents influenced the number of total hacking attempts as predicted in hypothesis H7. Persons with a higher risk propensity engaged in significantly more hacking attempts. Surprisingly, the level of rationality also exerted a significant influence on the number of total hacks. Hackers with a preference for analyt-

ic-rational thinking styles also committed significantly more attacks. One possible explanation for this finding is that, despite the higher risk awareness and the longer preparation times, hackers with a preference for analytic-rational thinking styles engage in more hacks simply because they are more successful in their hacks.

Table 16: OLS Regression Coefficients for estimated Effects of Rationality and Risk Propensity on Total Amount of Hacking Attacks

	Model 1			Model 2		
Variable	B	β		B	β	
Hypothesized characteristics						
Rationality index	174.60 *	.21	(74.72)	192.51 **	.23	(74.23)
Risk propensity index	228.44 ***	.33	(61.96)	243.44 ***	.35	(61.26)
Sociodemographic controls						
Age				-19.42	-.03	(68.87)
Female				16.69	.00	(1613.7)
Non-White				-17.10	-.00	(1279.4)
Education				-539.06	-.16	(368.80)
Marital status						
Living as married				1940.18	.16	(1073.5)
Married				510.49	.06	(956.86)
Unemployed				4110.45 **	.27	(1623.2)
Student				-2226.61 **	-.25	(829.90)
Constant	1981.59		(2215.30)	5438.62		(3345.22)
R-squared	.12			.29		

Note. Standard errors are listed in parenthesis.
*p<.05. **p<.01. ***p<.001.

Two of the sociodemographic control variables entered in the saturated model also exerted a significant effect on the number of hacks. Unemployed hackers reported a significantly higher number of hacking attacks than hackers who were employed (p<.01). One possible explanation for this finding could be related to the circumstance

that hacking is a time-consuming activity. Unemployed hackers simply have more time at their hands that they can dedicate to hacking. Time considerations could also be the reason why student hackers report to commit significantly fewer attacks ($p<.01$), since most of the students in the sample were part-time students who also had full-time jobs.

Overall, the regression analyses corroborated the hypotheses that were derived from the propositions of the rational choice perspective. With the exception of hypothesis H6, all predicted effects were found to be strongly significant and in the predicted direction in all models. The implications of these findings are discussed in the next chapter.

CHAPTER NINE:
DISCUSSION, IMPLICATIONS, AND LIMITATIONS

In the first section of the final chapter of this study, some of the main findings about hackers and the hacking community are summarized and briefly discussed. The chapter continues with a succinct discussion of the implications that the findings of this study hold for the application of the rational choice perspective to hackers. Next, some of the implications of this study for policy efforts to combat cybercrimes are discussed. The chapter concludes with a list of suggestions for future cyber-criminological research studies.

The (In)Accuracy of the Common Hacker Stereotype

The present study showed that the common hacker stereotype as a clever, lonesome deviant male adolescent whose computer proficiency compensates social shortcomings is barely beginning to tell the whole story of who hackers are. That is not to say that this stereotypical portrayal of hackers is completely mistaken. Several aspects of this characterization were indeed confirmed by the study results as well as the researcher's personal observations during the conference. First, the participants in this study were indeed highly educated, intelligent persons who had their inquiring minds set on technological developments. Many of these technophiles also seemed to be equally inventive, creative, and determined.

Second, the convention attendees were also predominantly males, and minority hackers were rare exceptions. The near uniformity with regard to the sex and race dis-

tributions, however, stood in sharp contrast to the strong emphasis of many attendees on an individualistic appearance. Many hackers conveyed their individualistic nature in conversations with the researcher as well as through their physical appearance. The physical expressions of individualism ranged from extravagant haircuts and hair colors, to unusual clothing styles, to large tattoos on various body parts, sometimes even on faces.

The two most important inadequacies of the hacker stereotype seem to be the notions that hackers are invariably young and that they are socially inept. The study found that hacking is by no means only a young man's game as Yar suggested (Yar, 2005a). It remains to be seen what fraction of hackers is actually comprised by teenagers, but the findings of this study clearly showed that persons of various age groups engage in hacking activities. More importantly, the data also revealed that hackers undergo a maturation process over the course of their hacking careers and that the more experienced and seasoned hackers tend to be the most dangerous ones. They are more likely to attack higher profile targets and some of them even engage in their illegal hacking activities with the stronger criminal intent of making financial profits.

Young and inexperienced hackers can certainly cause damage with their mischief, but the study showed that these hackers attack primarily private targets and do so out of intellectual curiosity, love for knowledge, experimentation, boredom, or youthful tomfoolery. Many hackers first became interested in hacking very early in their lives, and, typically, they were not driven by a pronounced initial criminal intent. As their hacking activities continued to become habitualized, however, many of them developed into more professional and ambitious hackers. Over the course of their hacking careers,

many intensified their hacking activities and began to also attack higher profile targets such as governmental and corporate information systems. Some hackers even reported having turned their once merely deviant juvenile behavior into a criminal business activity. A total of 15 percent of all respondents said that hacking had become their main source of income and that they would reject a target unless it was profitable. Undoubtedly, these experienced veteran hackers are the ones with whom law enforcement agencies should be most concerned about and to whom they should direct their attention.

Although the comparatively high fraction of unmarried hackers showed that many of them are indeed hesitant to engage in serious relationships and commitments, the vast popularity of social hacking methods and their high success rates also indicated that the commonly presumed social incompetence of hackers is wrong and misleading. The falseness of this assumption was further reaffirmed by some of the observations the researcher made during the convention. Most attendees appeared to be outgoing and sociable. Many attended the convention together with their friends, and most of the attendees seemed to share a distinct sense of humor and mingled quickly. Certainly, the informal observations during the convention and the findings that hackers are skilled in manipulating and 'programming' other persons and oftentimes manage to exploit the trust or carelessness of other computer users for their hacking purposes are not enough evidence for a strong rebuttal of the notion that hackers are social hermits. It might be the case that the sociability of hackers is limited to interactions with other, like-minded technophiles and that, although many appear to be skilled manipulators, genuine and affectionate social relations are of lesser importance to them. Additional examinations of

the social networks of hackers, their amount, frequency, and quality of interactions with close contacts, the types of contacts they engage in (face-to-face or online), and the importance they attribute to these social contacts are needed before a conclusion about the appropriateness of the assumption that hackers are recluses can be reached.

The debate about the sociability of hackers aside, one of the most important findings of the present study was the significant role of social hacking methods. The common perception of hacking attacks as being executed solely through technical means and the perception of hackers as socially incompetent are probably part of the reason why the danger posed by social engineering attacks is oftentimes underestimated. Unless these perceptions are revised and the awareness of social hacks is raised, social engineering methods will continue to be very successful and will pose a serious threat for many organizations.

The separate analysis of the three main hacking techniques in this study showed that many hackers combine social and technical methods and launch attacks that are comprised of both tactics. The examination of respondents who reported using both techniques in roughly equal amounts further revealed that they were the most successful hackers. Different from social and technical means and strategies, which appear to be commonly combined, the surveyed hackers largely refrained from distributing and spreading malicious code. Thereby, they demonstrated having a strong preference for directed attacks on selected targets over widely dispersed and randomly distributed attacks without specific targets. It appears that phishers, spammers, and virus coders are a group of cybercriminals that is distinctively different from ‘traditional’ hackers. Unfortunately, the limited amount of persons who distributed large amounts of malicious code

in the present study did not permit the analysis of whether these persons also exhibit other distinctive differences. More studies with larger subgroups of malware distributors are needed to draw such comparisons.

The Suitability of the Rational Choice Perspective

The discussion of the various theoretical difficulties facing the newly developing field of cyber-criminology in the fourth chapter expounded the main problems of transposing traditional, 'terrestrial' criminological theories to the online environment. The discussion established that the irrelevance of central assumptions of many traditional theories precludes their meaningful application to cybercrimes and cyber-criminals, and the violation of some traditional assumptions about offenders or other criminogenically relevant environmental aspects even renders some of them inapplicable to cybercrimes. As a result, the selection of potential theories is severely limited. The rational choice perspective was selected for the present study because it does not rest on any environment-specific assumptions and its main offender-related propositions are applicable to cyber-criminals. The results of this study suggest that the rational choice perspective is indeed a viable theory for the explanation and description of their behavior.

With only one exception, the hypotheses that were derived from the rational choice perspective were corroborated in the present study. The only hypothesis that received only partial support was the assumed effect of risk propensity on the length of preparations for hacking attacks. Nonetheless, the effect was found in the predicted direction and also reached a significant level in the second, saturated model. The analysis demonstrated the importance of the personality traits, rationality and risk propensity, for

various hacking-related decision-making processes and outcomes. Both traits were found to be influential factors on the overall success as a hacker, the length hackers take to prepare for their hacking attacks, the risk assessments of hackers, and the overall number of hacking attacks. The importance of rationality as a factor was further underlined by the finding that it was the most important factor in almost all regression models. The study established both factors as essential dimensions of cybercrime offender typologies.

The three involvement decision models of the rational choice perspective that were modified and transposed to fit the involvement in hacking proved to be suitable guidelines for the assessment of hacking-related decisions. While the study was not able to test all of the many factors thought to be influential for involvement in hacking, most of the examined factors were indeed found to be accurate. Some factors, however, deviated from the way they were proposed in the models. Most importantly, financial considerations were found to be irrelevant for the initiation phase. The model that was suggested in Chapter 3 emphasized financial needs, motives, opportunities, and inducements and it also considered employment to be relevant to the decision to engage in hacking activities. The results of this study, on the other hand, proved this assumption to be false. Different from other criminal activities, hackers seem to not be driven by financial considerations when they decide to begin to hack. Instead, the data documented that the importance of financial motivations as a driving motive for the continued involvement in hacking develops over time. Therefore, it should be included in the second model as one aspect of increased professionalism. With regard to considerations to desist from hacking, the study found risk-related deliberations to be most in-

fluential. Practical reasons were found to be of generally lower importance. The lower importance of practical reasons suggests that even if hackers find their hacking activities unsuited to yield a sustained income, they seem to continue to hack on a hobby basis. The decision to completely give up hacking, on the other hand, is most often made because hackers are afraid that their hacking activities could get them into trouble and jeopardize their careers in legitimate jobs and their lives.

Despite the general support for the theory that was found in this study, some of its drawbacks also became apparent. First, the generality of the principal propositions of the rational choice perspective rendered the deduction of precise hypotheses difficult. Only one of the six main propositions lent itself to meaningful and testable hypotheses. Furthermore, the testing of these hypotheses itself was found to be principally complicated because it had to resort either to psychological personality traits or to fictional scenarios. Second, the models that can be derived from propositions four to six, while evidently helpful in clarifying and structuring influential factors of the continued involvement in criminal activities, rest on many different causal assumptions that are exceedingly difficult to operationalize. Consequently, in order to account for the empirical specification of these models for the different types of crimes and offenders, the operationalization had to resort to univariate descriptions to determine the relative importance of the theoretically proposed factors and developments.

Rational choice perspective emphasizes the importance of two particular personality traits—the ability of offenders to deliberately weigh the outcomes of alternative actions and their willingness to take risks. Both factors, while corroborated as influential in the present study, do not lend exclusive support to the rational choice perspective.

The general theory of crime (Gottfredson & Hirschi, 1990) considers both personality traits as two of the six components that comprise low self-control. Future studies should examine all six dimensions of low self-control and investigate the influence of this personality construct on hacking activities. Furthermore, Jaishankar recently proposed the so-called space transition theory, the first criminological theory that was explicitly designed for the application to crimes committed in cyberspace (Jaishankar, 2008). Space transition theory provides an explanation for why otherwise law-abiding persons, who do not commit crimes in the terrestrial world, engage in cyber-criminal activities. It argues that people behave differently when they move from one space to another. Future cyber-criminological studies should devote special attention to this first exclusively cybercrime-related theory and test whether it is indeed better suited for the explanation of cybercrimes than traditional criminological theories.

The Policy Implications of the Study Findings

The conclusions that can be derived from this study are not limited to contributions to the scientific discourse about cybercrime offenders. They also hold some important implications for the efforts to combat cybercrimes. Experts agree that present efforts to combat cybercrimes are facing a multitude of challenges that have to be addressed. Aside from the resource shortages and other practical difficulties that were outlined in Chapter 3, law enforcement efforts to combat cyber-criminals are also hampered by a shortage of substantive and reliable information that can be used for the creation of cybercrime-offender profiles. Detailed profiles of the different types of cybercriminals, their skill levels, and their motivations are critical because they provide helpful

guidance for the investigation of cybercrimes and, thereby, increase the effectiveness of current prosecution efforts. A more effective response by the criminal justice system is urgently needed—not only because it would increase the number of convicted cybercriminals but, most importantly, because it would also have a preventive deterrence effect on the larger hacking community.

The findings of this study suggest that the creation of a deterrence effect has to become an essential component of efforts to combat cybercrimes. Unfortunately, present efforts to curb cybercrimes are hardly suited to exert a pronounced deterrence effect. Despite the annually increasing number of cybercrimes, only a relatively few high profile cybercrime cases are presently successfully tried, and many of them do not lead to swift or severe punishments (Brenner, 2006). The continuing unlikeliness of punishments is particularly problematic because it severely undermines any efforts to deter criminal behavior in cyberspace. Indeed, the findings of the present study demonstrate that many hackers are aware of the slim chances of being detected and punished. The current improbability of becoming prosecuted even led some hackers to report that they have never been afraid of being apprehended or prosecuted. Furthermore, the risk awareness of most hackers seems to decrease over time as they repeatedly learn that their actions have no negative consequences for them.

Nevertheless, several measures in this study also signify that deterrence can be a successful strategy to prevent cybercrimes. The study showed that many hackers have a nuanced risk awareness. For example, the majority of hackers report having become more concerned about risks in recent years, a finding that suggests that increased efforts to combat cybercrimes do not go unnoticed in the hacking community.

Furthermore, many hackers evidently distinguish between the chances of becoming detected and apprehended and the consequences of these two events. Most importantly, the data also indicate that the most successful hackers are the ones that also have the highest risk awareness. Thus, these hackers seem to be the ones that are most susceptible to changes in risk estimates.

Deterrence undoubtedly is an indispensable component in the control of all different types of criminal behaviors, but is seems to be particularly suited to prevent cybercrimes. Unlike other, less deliberately acting types of criminals, hackers plan their hacking attacks, and they oftentimes do so in an explicitly rational manner. Consequently, they should be more easily dissuaded than criminals who commit their crimes spontaneously whenever opportunities arise.

Taken together, the findings of this study suggest that a more pronounced deterrence perspective needs to become a central addition to the existing technical approaches to cybercrime prevention. However, merely adding deterrence as one separate component will not suffice. To be effective, a deterrence perspective has to be integrated into all currently existing national policy efforts to prevent computer crimes, ranging from legislation and regulation to law enforcement strategies. Moreover, it would also have to be implemented outside of national or state policies. One promising approach to establish deterrence policies in the private sector could be directed at businesses and organizations. The present study showed that most hackers pursue legal careers in legitimate jobs and companies. Organizations and companies that offer IT security services or are otherwise attractive to hackers should be encouraged to promote awareness of the potential consequences of committing cybercrimes. For exam-

ple, they could distribute information about punishments that have been given to convicted computer criminals as well as other informational materials that directly highlight what constitutes a crime under legal as well as ethical perspectives. Other informal control mechanisms, such as extra-legal social stigmata or the systematic introduction of negative effects on job opportunities might also be strong incentives to prevent particularly young middle-class computer experts from becoming involved in computer crime activities.

Unquestionably, the establishment of effective deterrence efforts as an integral part of cybercrime prevention strategies will not be an easy undertaking. The vast range of cybercrime activities and the multitude of different offenders considerably complicate the selections of the most appropriate deterrence policies. Strategies that are most effective for leisure-time juvenile hackers will most likely be unfit to deter destructive computer-security experts or other seasoned hackers from attacking computer systems for monetary gains. Nonetheless, deterrence should be pursued as a mitigation strategy, because even limited accomplishments can prevent some crime incidents and provide some protection from an increasingly serious problem.

Companies in branches that typically employ hackers can certainly be particularly helpful in deterring computer crimes, but the results of this study also indicate that all companies and organizations need to do more to actively prevent victimization, regardless of their branch. The analysis of the different hacking methods showed that, of all three main types of attack methods, social engineering attacks are the most successful ones. It also revealed that the various methods to obtain user passwords, be it the systematic guessing of weak or standard passwords or the theft of user logins remain the

most common ways hackers gain access to their targets. Moreover, the most successful hackers seem to launch combined hacking attacks that utilize both technical intrusion methods and information they obtained through social inquiries and deceptions of their victims. Thus, it seems that the weakest points of companies and organizations are their employees and members. Corporations have to educate their employees about social hacking methods. They need to raise awareness of the seriousness and frequency of the problem, educate their staff about the wetware tactics commonly used by hackers, and give them instructions of how to avoid becoming victimized.

The education of employers, while definitely an important protective measure, is not the only contribution that will be required from organizations. They also need to start reporting all their victimization incidents to the authorities. The current situation, in which individual organizations refrain from reporting incidents to protect their own interests and thereby harm the interest of all businesses, needs to be changed because, unless more incidents are reported, computer crimes are unlikely to become controllable. The benefits and detriments of a mandatory reporting system are debatable, but a reporting requirement would certainly benefit efforts to manage cybercrimes. It would put law enforcement agents in the position to decide which cases to devote their attention to rather than be dependent on the willingness of organizations to submit their cases in order to press charges.

The Limitations of the Present Study and Suggestions for Future Research

Even though it produced valuable insights into the sociodemographic composition of the hacking underground and the various developments hackers undergo over

the course of their hacking careers, the present study was limited in certain ways. One set of potential shortcomings relates to the sampling frame and the sample size of the study. The study analyzed only data from one particular convention, a circumstance that constricts the confidence with which the present findings can be generalized to larger populations. Although the ShmooCon convention attracted a diverse clientele, it remains unclear how general the profile of this particular convention really was. It also remains uncertain whether there are significant differences between the attendees of different conventions. More datasets from different conventions are needed to enable researchers to draw comparisons between them and to assess the reliability and validity of the present data. Once multiple studies from different conventions exist, meta-studies will eventually be able to compare the results of these studies and extract highly reliable and valid findings.

Although repeated studies from different conventions will eventually be able to generate valid and generalizable results, these results will, to a certain degree, be generalizable only to the subset of hackers who consider attending hacker conventions or, more narrowly, have already attended them. It remains to be seen whether there are systematic and consistent differences between hackers who potentially attend conventions and those who do not. The average age of respondents in this study, for example, was considerably higher than the typical age of hackers that other authors have suggested (Yar, 2005a). This finding indicates that studies operating with conventions as their sampling frames are indeed suffering from some systematic selection biases. An assessment of the exact areas in which such systematic differences exist and the degree to which they render the results of convention studies distinctively different from

other studies with different sampling frames can only be achieved by comparative studies. Until other sampling frames, such as message boards, have been utilized and until their results have been compared with the ones produced by convention studies, researchers have to remain cautious when generalizing convention-based study findings to all hackers.

Second, studies with larger sample sizes are needed to confirm some of the findings in the present study. The overall small sample size of this survey reduced the case numbers in some subgroups beneath commonly accepted margins of statistical generalizability. The regression results with regard to female hackers, minority hackers, and unemployed hackers, for example, have to be interpreted with the utmost caution and their validity should be reassessed with larger samples to verify their accuracy.

One important sample-size related aspect that has to be considered in this context is that, while larger sample sizes are certainly desirable, their creation bears practical problems. Despite the fact that the ShmooCon conference is one of the largest international hacker conventions, it was attended by 'only' about 800 persons, many of whom were not eligible for participation in the study. Accordingly, even though it achieved a relatively high response rate among eligible attendees, the present study yielded less than 130 cases. Two possible solutions for this problem come to mind.

First, researchers could solve this problem by collecting data from the world's largest hacking convention DefCon. DefCon is attended by over 7,000 persons and it also has a reputation for attracting many black hat hackers. The large size of this convention makes it the ideal candidate for studies that seek to obtain larger sample sizes. Researchers attempting to utilize the DefCon convention for their research purposes,

however, are most likely facing a different kind of challenge. DefCon has a reputation of being a less professional convention and a convention that is attended by many hackers mainly to enjoy a fun weekend in Las Vegas with like-minded people. The resulting challenge for potential research projects is to conduct the study before attendees become intoxicated and no longer take the research project seriously.

An alternative solution for the sample-size problem would be to combine the datasets from different conventions. The results from different studies of various conventions could be merged into one larger dataset. Although this approach promises to provide larger case numbers and will likely yield generalizable results, it is not without disadvantages. The individual surveys would have to repeatedly ask the same item subsets to be comparable, thus hindering and delaying the assessment of different hacking-related aspects and the development of more advanced survey instruments.

Aside from potential biases resulting from the sampling frame and the problems associated with the small sample size, it is reasonable to assume that the present research project was also confronted with the problem of social-desirability biases. Social-desirability biases are introduced through the propensity of respondents to give socially desirable responses. They are a common problem of studies that rely on indirect, subjective information provided by respondents rather than objective or direct measures, or a combination of the two (Fisher, 1993). In the case of cyber-criminals, social-desirability biases are extremely difficult to overcome because objective measures of cybercriminal activities are difficult to obtain. One possible assessment of social-desirability biases could be achieved by conducting a research study that combines a survey section with a direct measurement of hacking skills and expertise. For example,

a honeypot could be used as one possibility to obtain a direct measurement. In computer terminology, the term 'honeypot' refers to a forensic software trap which can, among other things, be used to log and analyze hacking activities. This honeypot environment could be utilized to verify the skill levels respondents claim to have. The inclusion of such a direct measurement, however, complicates the study and the obtainment of IRB approval and significantly increases the effort for respondents. For that reason, the conduction of such a combined study during a convention is highly unfeasible.

The present study was a first attempt to generate quantifiable information about the hacking underground, and, as such, it was also naturally limited with regard to how many aspects of this community were assessable. As does every extension of our knowledge, the current study provided some answers but also raised many more questions. Future studies need to include other measurements of attitudes, social networks, personal background information, and many other aspects to refine and extend our understanding of hackers. Such studies could specify and detail many additional characteristics in a more precise way. The large fraction of college-educated hackers in this study, for example, rendered the educational achievement variable close to a constant. To better assess the impact of varying educational backgrounds, future studies could ask respondents what their study subject is or was and what type of college they attend(ed). The same is true for the measures of employment, to name but a second aspect. It would be interesting to know the exact profession of respondents and whether and how their occupations are related to their hacking activities.

Although the paper-pencil format was, for several practical reasons, the only viable design of the present study, this format was not ideally suited for the assessment of

the great diversity of different types of hackers. Electronic computer-based surveys should be designed for future studies because they allow more complex path dependencies and, thus, are better able to capture the wide range of different types of hackers. For example, such surveys could begin by asking respondents whether they identify themselves as white or as black hat hackers and then ask different sets of questions for each type of hacker. Studies operating with such measurement techniques would be geared more specifically to the different types of hackers and would yield more detailed and more encompassing results without systematically excluding any type of hackers. Thereby, they could provide answers to pressing questions such as what exactly the ratio between white hat and black hat hackers is, and what fraction of the hacking community is comprised by law-abiding white hat hackers and penetration testers. They could also assess tensions within the hacking community by revealing the attitudes and opinion white hat and black hat hackers have about each other. Our understanding of the hacking underground is just beginning to evolve and such studies could add much needed details.

While the survey format of the present study was appropriate to address the main components and factors of the involvement decisions as proposed by rational choice perspective, its ability to capture the intricacies of event decisions was limited. Thus, aside from the various types of surveys suggested above, cybercrime researchers should also conduct more event specific studies or analyze forensic crime science protocols to better capture and reconstruct the intricate decision-making processes that are involved in such complex events.

Parallel to analyzing the various personality traits that influence the behavior of hackers, cybercrime researchers should further begin to construct typologies of different hacker profiles. The multitude of motives and skills that were confirmed by this study suggests that a variety of different types of hackers exist. Researchers should attempt to isolate prototypical types of hackers, construct typologies of the various types, collect empirical evidence to ensure the included types of hackers are exhaustive and mutually exclusive, and examine how exactly the various types of hackers differ from and relate to each other.

The long list of future studies that were suggested in this last section calls to mind that cyber-criminology is only just beginning to develop and that our knowledge about cybercrime offenders remains fragmentary at best. The present study yielded some important insights into the composition of the hacking underground and it shed some light on the motivations and maturation processes of hackers. Nevertheless, it was but one step toward the establishment of cyber-criminology as a distinct subfield of criminological research. A long and difficult road is still ahead for this young field of criminological research.

APPENDIX A:
THE SURVEY QUESTIONNAIRE

Hacking Questionnaire 2008

Hello and thank you for your willingness to participate in this survey!
My name is Michael Bachmann and I am a student at University of Central Florida doing a study about hackers and their hacking activities.

First, let me assure you that:
- The survey is **strictly noncommercial** and for my **private dissertation research only**.
- There are **no institutions or organizations involved** in or affiliated with this project.
- All information is **completely anonymous, confidential** and your participation is **voluntary**.
- Completion of this survey takes about **15 minutes**.
- It is for **research purposes only**.

OK, let's begin:

First, let me ask you some questions about your hacking activity in general.

01 Are you currently actively hacking?

☐ Yes ☐ No

If you answered this question with no, please think back to when you were still hacking when answering the questions below.

---

02 At approximately what age did you begin to become interested in hacking? _____

---

03 What were your initial motivations to become interested in hacking? (Mark all that apply)

☐ Intellectual curiosity	☐ Excitement, thrill, fun	☐ Experimentation
☐ Status and prestige	☐ Financial gain	☐ Peer recognition
☐ Political Ideology	☐ Media attention	☐ Protest against corporations
☐ Self-concept boost	☐ Feeling of power	☐ Personal revenge

☐ Other (specify) _____

---

04 What would you say was your primary motivation? (select one answer from question 3)

_____

---

05 How long was the timeframe between your initial interest and your first actual hack?

_____ Days _____ Weeks _____ Months _____ Years

06 What were the initial motivations for your first hack? (Please mark all that apply)

☐ Intellectual curiosity ☐ Excitement, thrill, fun ☐ Experimentation
☐ Status and prestige ☐ Financial gain ☐ Peer recognition
☐ Political Ideology ☐ Media attention ☐ Protest against corporations
☐ Self-concept boost ☐ Feeling of power ☐ Personal revenge
☐ Other (specify) _____

---

07 What was the type of target of your first hack?

☐ Private single host ☐ Private network ☐ Private website
☐ Corporate single host ☐ Corporate network ☐ Corporate website
☐ Non-profit single host ☐ Non-profit network ☐ Non-profit website
☐ Government single host ☐ Government network ☐ Government website
☐ Other (specify) _____

---

08 Based on which criteria did you select your first target?

☐ Easy access ☐ Interesting information ☐ Profitable information
☐ Reputation gain ☐ Antipathy ☐ Other (specify) _____

---

09 Were you employed when you first started to hack?

☐ Yes, full-time ☐ Yes, part-time ☐ No

---

10 Was economic profit a motivation at all?

☐ Yes, an important one ☐ Yes, but not very important ☐ No

---

11 What methods did you use in your first technical intrusion? (Please mark all that apply)

☐ Footprinting ☐ Ping sweeping ☐ DNS zone transfer
☐ Whois ☐ Network mapping ☐ Port scanning
☐ Versatile scanning tools ☐ Vulnerability scanning ☐ RPC port/end-point dump
☐ Packet sniffing ☐ Session hijacking ☐ Grinding Passwords
☐ Password cracking ☐ Password theft ☐ Directory traversal/climbing
☐ Buffer overflow ☐ Format string ☐ Resource mismatch
☐ CGI ☐ Root shell/kits ☐ Keylogger
☐ Spoofing ☐ Bouncing ☐ Source routing
☐ Other (specify) _____

---

12 Approximately how often have you attempted technical intrusions in your life? _____ times

13 How frequently do you attempt technical intrusions?

_____ Per Week or _____ Per Month or _____ Per Year

---

14 Approximately how many of them are successful?

☐ 0% ☐ 10% ☐ 20% ☐ 30% ☐ 40% ☐ 50% ☐ 60% ☐ 70% ☐ 80% ☐ 90% ☐ 100%

---

15 Have you ever used "WetWare" social methods? (Please mark all that apply)

☐ Social Engineering ☐ Deception ☐ Bribery

☐ Shoulder Surfing ☐ Impersonation ☐ Dumpster diving

---

16 Approximately how often have you attempted social methods in your life? _____ times

---

17 How frequently do you attempt social methods?

_____ Per Week or _____ Per Month or _____ Per Year

---

18 Approximately how many of them are successful?

☐ 0% ☐ 10% ☐ 20% ☐ 30% ☐ 40% ☐ 50% ☐ 60% ☐ 70% ☐ 80% ☐ 90% ☐ 100%

---

19 Have you ever distributed? (Please mark all that apply)

☐ Trojan Horses ☐ Adware/Spyware

☐ Viruses/Worms ☐ Spam/Phishing mails

☐ None of the above ☐ Other (specify) _____

---

20 Approximately how often have you distributed malware in your life? _____ times

---

21 How frequently do you distribute malware?

_____ Per Week or _____ Per Month or _____ Per Year

---

22 How successful would you say you were with your distributions?

☐ ☐ ☐ ☐ ☐ ☐ ☐

Not at all Somewhat Very

---

23 Approximately how long have you been hacking now? _____ Months _____ Years

---

24 Did you change friends and peers since your first hack to include more other hackers?

☐ Yes, very much ☐ Yes, somewhat ☐ No

25 Would you say you have improved your skills since your first hacking attempts?

☐ Yes, very much ☐ Yes, somewhat ☐ No

---

26 Has your hacking activity become more frequent since your first hacking attempts?

☐ Yes, very much ☐ Yes, somewhat

☐ No, it's the same ☐ No, it's less frequent

---

27 Have your motivations changed since your first hacking attempts?

☐ Yes, very much ☐ Yes, somewhat ☐ No

---

28 Currently, what is your main motivation for hacking? (specify): _____

---

29 Have your targets changed since your first hacks?

☐ Yes, very much ☐ Yes, somewhat ☐ No

---

30 Would you say your targets have become higher profile targets?

☐ Yes, very much ☐ Yes, somewhat ☐ No

---

31 What is the type of target you currently prefer?

☐ Private single host ☐ Private network ☐ Private website

☐ Corporate single host ☐ Corporate network ☐ Corporate website

☐ Non-profit single host ☐ Non-profit network ☐ Non-profit website

☐ Government single host ☐ Government network ☐ Government website

☐ Other (specify) _____

---

32 What are your current selection criteria for targets?

☐ Easy access ☐ Interesting information ☐ Profitable information

☐ Reputation ☐ Antipathy ☐ Other (specify) _____

---

33 What might be a reason for you to reject a potential target? (Please mark all that apply)

☐ Unfamiliarity with architecture ☐ No interesting information

☐ No profitable information ☐ Sympathy with host

☐ None of the above ☐ Other (specify) _____

---

34 Have your methods and tactics changed since your first hack?

☐ Yes, very much ☐ Yes, somewhat ☐ No

35 What is your currently preferred method and tool for the different stages of a hack?
(Please write in what you prefer to use for each of the following stages)

Reconnaissance: _____

Gaining access: _____

Persisting: _____

Propagating: _____

Paralyzing: _____

Covering up: _____

---

36 Do you follow a persistent pattern in all your hacks or do you vary or change your methods?

☐ ☐ ☐ ☐ ☐ ☐ ☐

Very persistent pattern Vary a lot

---

37 Do you have preferred tools you use in all your hacks or do you vary your software tools?

☐ ☐ ☐ ☐ ☐ ☐ ☐

Always same tools Vary tools a lot

---

38 Which methods do you employ to remain anonymous? (Please mark all that apply)

☐ Spoofing ☐ Bouncing ☐ Source routing

☐ Proxies ☐ TOR, I2P, etc. ☐ Tunnels, Covert channels

☐ War driving ☐ Public access points (e.g. Internet cafes)

☐ Other (specify) _____

---

39 Is hacking a source of any income for you?

☐ Yes, the main ☐ Yes, but not the main ☐ No

---

40 Have you ever thought about quitting hacking?

☐ Yes, often ☐ Yes, a few times ☐ Never

---

41 If yes, what caused you to question continuing to hack? (Please mark all that apply)

☐ Involved risk ☐ Involved effort ☐ Income too irregular

☐ Fear of detection ☐ Fear of apprehension ☐ Fear of prosecution

☐ Legal alternatives ☐ Other (specify) _____

---

42 Are you more/less afraid of being traced, tracked, or apprehended then when you started?

☐ More afraid ☐ Less afraid ☐ Unchanged ☐ I was never afraid

43 How much time do you usually invest in preparation, planning, considering routes of action, selection of techniques and tools?

_____ Hours _____ Days _____ Weeks _____ Months

---

44 Do you spend more or less time for planning today than when you started to hack?

☐ More time today ☐ About the same time ☐ Less time today

---

45 Please estimate the risk you run of being detected during/after a hack.

☐ ☐ ☐ ☐ ☐ ☐ ☐

No risk at all Some risk Very high risk

---

46 Please estimate the risk you run of being apprehended during/after a hack.

☐ ☐ ☐ ☐ ☐ ☐ ☐

No risk at all Some risk Very high risk

---

47 Approximately what percentage of attacks have you aborted because you were afraid of detection?

☐ 0% ☐ 10% ☐ 20% ☐ 30% ☐ 40% ☐ 50% ☐ 60% ☐ 70% ☐ 80% ☐ 90% ☐ 100%

---

48 During the hacks, do you tend to focus more on the potential rewards or the potential risks?

☐ ☐ ☐ ☐ ☐ ☐ ☐

Only on rewards Balance both Only on risks

---

49 Would you say you act rational and deliberate during your hacks or do you sometimes get caught-up in the moment and act emotionally?

☐ ☐ ☐ ☐ ☐ ☐ ☐

Very rational Very emotional

Now, please indicate how much you agree or disagree to the following statements (you are almost finished):

50 I always try to avoid situations involving a risk of getting into trouble.

☐ ☐ ☐ ☐ ☐ ☐ ☐

Strongly disagree Strongly agree

---

51 I always play it safe even when it means occasionally losing out on a good opportunity.

☐ ☐ ☐ ☐ ☐ ☐ ☐

Strongly disagree Strongly agree

---

52 I am a cautious person who generally avoids risks.

☐ ☐ ☐ ☐ ☐ ☐ ☐

Strongly disagree Strongly agree

53 I am rather bold and fearless in my actions.

☐ ☐ ☐ ☐ ☐ ☐ ☐

Strongly disagree Strongly agree

---

54 I am generally cautious when trying something new.

☐ ☐ ☐ ☐ ☐ ☐ ☐

Strongly disagree Strongly agree

---

55 I usually have clear, explainable reasons for my decisions.

☐ ☐ ☐ ☐ ☐ ☐ ☐

Strongly disagree Strongly agree

---

56 I don't reason well under pressure.

☐ ☐ ☐ ☐ ☐ ☐ ☐

Strongly disagree Strongly agree

---

57 Thinking hard and for a long time about something gives me little satisfaction.

☐ ☐ ☐ ☐ ☐ ☐ ☐

Strongly disagree Strongly agree

---

58 I prefer complex to simple problems.

☐ ☐ ☐ ☐ ☐ ☐ ☐

Strongly disagree Strongly agree

---

59 I enjoy solving problems that require hard thinking.

☐ ☐ ☐ ☐ ☐ ☐ ☐

Strongly disagree Strongly agree

---

60 Using my gut-feelings usually works well for me in working out problems in my life.

☐ ☐ ☐ ☐ ☐ ☐ ☐

Strongly disagree Strongly agree

---

61 I trust my initial feelings about situations.

☐ ☐ ☐ ☐ ☐ ☐ ☐

Strongly disagree Strongly agree

---

62 I like to rely on my intuitive impressions.

☐ ☐ ☐ ☐ ☐ ☐ ☐

Strongly disagree Strongly agree

---

63 I often go by my instincts when deciding on a course of action.

☐ ☐ ☐ ☐ ☐ ☐ ☐

Strongly disagree Strongly agree

64 I don't think it is a good idea to rely on one's intuition for important decisions.

☐ ☐ ☐ ☐ ☐ ☐ ☐

Strongly disagree Strongly agree

Finally, let me ask you some general questions about yourself.

65 What is your gender?

☐ Male ☐ Female

---

66 What year were you born? 19__

---

67 What is the last grade or class you completed in school?

☐ None, or grades 1-8

☐ High school incomplete (grades 9-11)

☐ High school graduate (grade 12 or GED certificate)

☐ Business, Technical, or vocational school AFTER high school

☐ Some college, no 4-year degree

☐ College graduate (B.S., B.A., or other 4-year degree)

☐ Post-graduate training/professional school after college (Master's degree or Ph.D.)

---

68 Are you, yourself, of Hispanic or Latino origin or descent, such as Mexican, Puerto Rican, Cuban, or some other Spanish background?

☐ Yes ☐ No

---

69 What is your race?

☐ White ☐ Black ☐ Asian ☐ Other mixed race: (specify) _____

---

70 Are you married, living as married, divorced, separated, widowed, or never been married?

☐ Never been married ☐ Living as married ☐ Married

☐ Divorced ☐ Separated ☐ Widowed

---

71 Are you now employed full-time, part-time, retired, or not employed for pay?

☐ Employed full-time ☐ Employed part-time

☐ Not employed for pay ☐ Retired

---

72 Are you also a full- or part-time student?

☐ Yes, full-time ☐ Yes, part-time ☐ No

Thank you very much for your time! Have a nice day and enjoy the rest of the conference.

APPENDIX B:
THE SURVEY CONSENT FORM

What Makes Them Click? Hacking Experiences and the Decisions Involved in Hacking

Michael Bachmann, Principal Investigator

Informed Consent Form

I am a sociology Ph.D. student at the University of Central Florida (UCF). This survey is part of my dissertation research which explores general hacking experiences and the involved decision-making processes. Your participation will address these issues and involves you and other consenting attendees of this conference.

You will be asked questions about your hacking experiences, your motivations, methods, and decision-making processes. Altogether, the survey takes only around fifteen minutes.

The primary purpose of this study is to further our understanding and knowledge of hackers and the hacking community, a group that has so far been largely ignored by sociological researchers. The study does not include any potential risk for participants because it contains no identifiers, is completely anonymous, and asks only general questions about hacking activity. It does not collect any specific illegal or self-incriminating information.

You are free not to answer any question you choose not to answer. You are free to end the survey at any time. Deciding not to answer questions or to end the survey altogether will not affect your status as an attendant of this conference in any way. Your participation in this research is completely voluntary.

This research is governed by a privacy certification that prohibits the researcher from disclosing any individual information to any outside party, including other attendees of this conference. All information you provide in the survey is completely anonymous and will be kept in the strictest confidence by the researcher. The researcher cannot divulge any information and no information can be linked specifically to you.

Questions

Please feel free to ask any questions you want before you fill out the survey or at any time during the survey. If you feel that I have not adequately answered all your questions, contact my faculty supervisor Dr. Harold J. Corzine (407) 823-2202. You may call that number but be sure to identify yourself as a participant in the hacking study.

Your consent

I understand the basic procedure of this study and am aware that I may discontinue participation at any time. I hereby consent to participate in a survey of about fifteen minutes that focuses on general hacking experiences.

I understand that this study is anonymous, confidential, strictly non-commercial, and for dissertation research purposes only. Only the researchers will have access to the questionnaire. No other person or organization, including other attendees at this conference will have access to my questionnaire. I understand that I must be at least 18 years old to participate in this research project. I understand that my participation or non-participation in this study has no bearing one way or the other on my status as an attendee of this conference. I understand that no compensation can be provided for my participation in this study.

If you believe you have been injured during participation in this research project, you may file a claim against the State of Florida by filing a claim with the University of Central Florida's Insurance Coordinator, Purchasing Department, 4000 Central Florida Boulevard, Suite 360, Orlando, FL 32816, (407) 823-2661. University of Central Florida is an agency of the State of Florida and the university's and the state's liability for personal injury or property damage is extremely limited under Florida law. Accordingly, the university's and the state's ability to compensate you for any personal injury or property damage suffered during this research project is very limited.

Information regarding your rights as a research volunteer may be obtained from:

Barbara Ward, CIM
Institutional Review Board (IRB) Coordinator
University of Central Florida (UCF)
Office of Research & Commercialization
12201 Research Parkway, Suite 501
Orlando, Florida 32826-3246
Telephone: (407) 823-2901

You do not need to sign this consent form. Submission of a completed questionnaire constitutes your consent to participate in this research project.

APPENDIX C:
THE IRB APPROVAL LETTER

University of Central Florida Institutional Review Board
Office of Research & Commercialization
12201 Research Parkway, Suite 501
Orlando, Florida 32826-3246
Telephone: 407-823-2901, 407-882-2012 or 407-882-2276
www.research.ucf.edu/compliance/irb.html

Notice of Exempt Review Status

From: **UCF Institutional Review Board**
FWA00000351, Exp. 5/07/10, IRB00001138

To: **Michael Bachmann**

Date: **February 05, 2008**

IRB Number: **SBE-08-05422**

Study Title: **What Makes Them Click? Hacking Experiences and the Decisions Involved in Hacking**

Dear Researcher:

Your research protocol was reviewed by the IRB Chair on 2/4/2008. Per federal regulations, 45 CFR 46.101, your study has been determined to be **minimal risk for human subjects and exempt** from 45 CFR 46 federal regulations and further IRB review or renewal unless you later wish to add the use of identifiers or change the protocol procedures in a way that might increase risk to participants. Before making any changes to your study, call the IRB office to discuss the changes. **A change which incorporates the use of identifiers may mean the study is no longer exempt, thus requiring the submission of a new application to change the classification to expedited if the risk is still minimal.** Please submit the Termination/Final Report form when the study has been completed. All forms may be completed and submitted online at https://iris.research.ucf.edu.

The category for which exempt status has been determined for this protocol is as follows:

2. Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey or interview procedures, or the observation of public behavior, so long as confidentiality is maintained.

(i) Information obtained is recorded in such a manner that the subject cannot be identified, directly or through identifiers linked to the subject, **and/or**

(ii) Subject's responses, if known outside the research would not reasonably place the subject at risk of criminal or civil liability or be damaging to the subject's financial standing or employability or reputation.

A **waiver of documentation of consent** has been approved for all subjects. Participants do not have to sign a consent form, but the IRB requires that you give participants a copy of the IRB-approved consent form, letter, information sheet, or statement of voluntary consent at the top of the survey.

All data, which may include signed consent form documents, must be retained in a locked file cabinet for a minimum of three years (six if HIPAA applies) past the completion of this research. Any links to the identification of participants should be maintained on a password-protected computer if electronic information is used. Additional requirements may be imposed by your funding agency, your department, or other entities. Access to data is limited to authorized individuals listed as key study personnel.

On behalf of Tracy Dietz, Ph.D., UCF IRB Chair, this letter is signed by:

Signature applied by Janice Turchin on 02/05/2008 11:23:13 AM EST

Janice M Turchin

IRB Coordinator

GLOSSARY

ARPANET

A network created in 1969 by the US Defense Department's Advanced Projects Research Agency (ARPA) to develop a system of data communications for scientific and military operations. ARPANET adopted the TCP/IP communications standard, which defines data transfer on the Internet today.

Black Hats

Hackers (more correctly called crackers) who engage in destructive computer exploits, motivated by greed, revenge, sabotage, blackmail, that can result in harm to property and/or to people.

Bouncing

Bouncing is a method similar to spoofing. The attacker uses proxy servers or computers to relay, or bounce, their requests to the attacked machines and to evoke the impression the attack originated from the address it was channeled through.

Buffer

A region of memory set aside to temporarily store output or input data waiting to be directed to a device.

Buffer Overflow

In computer security and programming, a buffer overflow, or buffer overrun, is a programming error which may result in a memory access exception and program termination, or in the event of a malicious attack, a breach of system security.

CGI

CGI (Common Gateway Interface) denotes an interface program that enables an Internet server to run external programs to perform specific functions, such as creating “dynamic” content. Several broad-spectrum scanners exist that detect known vulnerabilities in CGI programs. CGI attacks are among the most popular attack methods on Internet servers. Most website defacements exploit the CG Interface.

Cracking

Gaining unauthorized access to computer systems to do harm or commit a crime.

Cracker

Cracker is a label for a malicious black hat hacker who breaks into remote computer systems without authorization in order to commit crimes.

Cybercrime

A crime related to technology, computers, and the Internet, resulting in harm to property and/or persons.

Cyberspace

Composed of millions of interconnected computers, servers, routers, switches, and fiber optic cables, cyberspace allows critical infrastructures to work. Today, it is the nervous system of the global economy.

Directory Traversal/Climbing

Directory traversal or directory climbing, sometimes also referred to as backtracking, denotes one of the most common exploits on the Internet. By altering the

path of an URL, the attacker is reading files from a website that are not intended to be shared over the Internet.

DNS

DNS stands for Domain Name System, a computer program running on web servers that translates URL domain names into IP addresses in order to direct easy-to-remember domain name requests (e.g. http://www.google.com) to the respective binary IP address (216.239.39.99) of the domain host.

DNS Zone Transfer

DNS, or Domain Name System, is a program that is used by DNS servers to translate user-friendly Uniform Resource Locator (URL) domain names (e.g. http://www.google.com) into the respective binary IP address (in the case of http://www.google.com the number 216.239.39.99) of the domain host. When receiving such a request, DNS servers look for the domain name in their database and direct the request to the IP address associated with that domain name. Most of the queries that are received by Domain Name Systems request translations of URL domain names into IP addresses. The functionality of the Domain Name System, however, is not limited to such translations. One additional feature of DNS servers is the so-called “Zone Transfer”. The Zone Transfer feature allows downloading the entire table of names and IP addresses contained within a network from the DNS database. Downloading this table enables the hacker to effectively map a network. Typically, the information contained in the database reveals the IP addresses of hosts that are likely to be active as well as the location of important servers and sometimes even user names. DNS Zone Transfers are

typically used to spy out lower profile and lesser-secured target networks because many professional network administrators disable the Zone Transfer functions of their DNS servers or ensure that no compromising information is sent out through such transfers.

Dumpster Diving

Dumpster diving is a slang term for searching through somebody's garbage. For attackers, this search can be a legal and powerful source of information because many people do not destroy sensitive information before their disposal due to social taboos.

Footprinting

Sometimes also referred to as fingerprinting, is a term that can have two meanings. Sometimes footprinting is equated with reconnaissance tactics. In this understanding, all different kinds of activities aimed at gathering information about computer systems, networks, or websites, and the entities they belong to are subsumed under this term. When equated with the reconnaissance phase, footprinting commonly involves a range of technical methods, such as ping sweeps, port scans, operation system identifications, network enumerations, registrar queries, and many others. The second, more common understanding of the term is of a much more narrow scope and denotes one specific activity, namely, the identification of a particular operation system through the interpretation of specific responses of a computer system that reveal the identity of that particular system. In order to trigger the system to reveal identifying responses, the attacker submits unexpected combinations of code to the target. While most systems respond

in the same way to correct response requests, they rarely respond the same way to requests that the programmers could not anticipate. A Windows Vista operation system, for instance, responds to faulty data requests in a way that is distinctively different from a Mac OS, a UNIX OS, a prior Windows OS, or any other kind or operation system. Thus, footprinting techniques allow the hacker to identify the exact host computer system or platform he or she is targeting and allows him or her to gear the attack towards the specific vulnerabilities of that particular system. Footprinting techniques allow the hacker to identify the exact host computer system or platform he or she is targeting and allows him or her to gear the attack towards the specific vulnerabilities of that particular system. The method is used for attacks on individual hosts and networks as well as websites, because it also allows the hacker to identify weaknesses and points-of-entry in the operation system of a server that hosts the targeted website. Footprinting is used by hackers of different skill levels. Whereas lesser skilled attackers will resort to readily available footprinting tools, attackers having the necessary programming knowledge typically prefer to use their own, custom-made footprinting requests.

Format String

Format strings denote an attack method similar to buffer overflows. By programming input with special formatting codes, attackers can override memory areas on a target host and use this memory for crashing the program, get access to information from different locations in the computer's memory, or even for breaking into the host system.

Grinding Passwords

The act of remotely guessing login passwords is oftentimes referred to as grinding passwords. The attacker continually logs on remote machines and guesses a different password each time. Alternatively, the hacker can attempt to log onto many different machines with the same commonly used password.

Hacker

A person who enjoys learning the details of computer systems and how to stretch their capabilities. In the public discourse, hacker is often used synonymously with the term cracker.

Honeypot

In computer terminology, a honeypot is a trap set to detect, deflect, or in some way counteract attempts of unauthorized intrusions.

I2P

I2P, originally also termed the Invisible Internet Project, is an anonymous network that can be used for anonymous surfing and to transfer files anonymously.

ICMP

ICMP stands for “Internet Control Message Protocol”, an integral part of the Internet Protocol that handles error and control messages. Routers and hosts use ICMP to send reports of problems about data packets back to the originating source.

IP address

Internet Protocol, or IP, addresses uniquely identify a computer accessible over a TCP/IP-based network or the internet in a four-part numerical format.

Keylogger

Once an attacker has successfully gained access to a target system, he typically installs packet sniffers to record network communications and keyloggers to record all keystrokes users of that system enter on the keyboard. Several versions of keyloggers exist for special purposes such as, for example, recording only passwords.

LAN

Local Area Network: A user-owned and operated data transmission network that typically connects a number of communicating devices such as computers, routers, gateways, terminals, or printers located within a small geographical area. LANs are typically distinguished from WANs, Wide Area Networks such as the Internet, which span very large geographical areas or even the entire world.

Network Mapping

While ping sweeps provide the attacker with the addresses of active remote hosts, they do not provide any information about the networks these hosts are located in. In order to explore and document the layout of a network, its topology, traffic paths, structures, services, and its performance between nodes, attackers typically use additional tools. Among the oldest and simplest of these tools is traceroute, a utility that displays the times and locations of intermediate stops along the route data packets travel to reach their destination. Modern network mappers oftentimes combine a vast array of powerful and versatile utilities that allow users to identify a multitude of network details, among them active hosts and open ports, running applications and services, the rules of firewalls within the network,

and even the contents of data packets sent within the network. While network scanning is often done with such versatile scanning tools, it is not limited to only such utilities. Typically network mapping tools are used in attacks against networks or specific hosts located within those networks. The basic skill level required to perform a network scan is not high, but network scans of more experienced hackers can be sophisticated and performed with advanced and customized tools. Three main subcategories of network scans exist that were asked separately in the questionnaire: port scanners, versatile scanning tools, and vulnerability scanners.

Packet

A piece of data of fixed or variable size that is sent through a communication network like the Internet. A message is typically broken up into packets before it is sent over a network.

Packet Sniffing

Packet sniffing is the computer equivalent of wire-tapping a telephone communication. Sniffing programs disable the filter of Ethernet cards, thus allowing them to monitor all communication within a network.

Password Cracking

Password cracking is the act of decrypting and recovering the passwords stored on a computer system. Every system has to store passwords to be able to authenticate users. Password crack utilities are used to decipher the encryption and reveal the account passwords to the attacker.

Password Theft

Password theft is one of the simplest and oldest hacking methods. Once the legitimate username and password are known, the attacker can exploit the user account without having to worry about any countermeasures such as firewalls or intrusion detection systems because they cannot distinguish between the legitimate user and the attacker.

Phreaking

Phreaking is a slang term coined to describe the activity of a subculture of people who study, experiment with, or explore telephone systems, the equipment of telephone companies, and systems connected to public telephone networks. Oftentimes, phreaking denotes the act of breaking into a telephone network for the purpose of making free calls or to charge calls to another person's account.

Ping

Ping is the short version for Packet Internet Groper, a utility that sends out data packets to check whether a remote host is currently connected to a LAN network or the Internet and to test the quality of the connection to that remote host. The utility sends out ICMP “echo request” packets to the target host and listens for ICMP “echo response” replies. The tool then estimates the round-trip time between sending the request and receiving the response and records any packet loss in a statistical summary.

Ping Sweeping

The term “ping sweeping,” sometimes also referred to as Internet Control Message Protocol (ICMP) sweep, denotes a basic network scanning technique used

to determine the IP addresses of active, or live, hosts within a network. Whereas single ping commands are used to determine the network location and availability of one particular remote computer host, a ping sweep consists of ICMP “echo request” packets that are send to multiple hosts within one IP address range or entire network. All currently available hosts within the scanned range will reveal their availability through returned “echo replies”, which are typically summarized by the ping sweeping tool in a list of all active IP addresses within the specified address range. Ping sweeps are typically used in attacks against networks, but they can also be used to identify one specific target host within a network. They do not require a high level of sophistication, are among the dated and slower network scanning methods, and suffer from two main drawbacks. Ping sweeps are detectable and will alert professional network technicians of an imminent attack. Also, many network administrators sometimes simply block ICMP echo requests being sent from their networks, in which cases the attacker then has to resort to scanning open TCP ports. Since they bear some danger of compromising the attack and reveal only limited amounts of information, ping sweeps are commonly used by lesser skilled hackers and in combination with other network scanning methods. They are contained in many popular network scanners such as nmap, nessus, and others, and their execution does not require a high level of sophistication. To the contrary, the execution of a ping sweep is relatively simple and merely requires the attacker to know the range of the targeted IP addresses.

Port

In the context of TCP/IP and UDP based computer networks, the term port refers to an end point of a logical service connection that is numerically identified between 0 and 65536. For example, port 80 is used for HTTP traffic.

Port Scanning

Just as network scanners, port scanners are commonly used by network administrators to test the security of their networks and by hackers to compromise it. In order to understand how exactly a port scan works and why many hacking exploits rely on open ports, it is import to know what a port is. Ports are one of the main two components of the common Internet protocol TCP/IP. Within the TCP/IP protocol, the destination of a data packet is determined by two components, the destination address of the computer the packet is sent to and the destination port for the particular type of data packet. Even though firewalls close the majority of ports on most computers, specific ports or ranges of ports have to remain open for services and applications that are running on a host to be able to receive incoming information. Two vulnerabilities, in particular, are associated with open ports: security concerns associated with the program responsible for delivering the service and with the operating system running on the host. Port scanners allow an attacker to scan a range of listening ports on a target host for ports that are open and can be used as entry points to this host. Port scanners are commonly used in a variety of different hacking attacks, and they do not require a high level of sophistication. The successful exploitation of open ports is a more difficult undertaking than their mere detection in a scan.

Proxy

In the context of computer networks, proxies are gateways that relay one Internet session to another. Many proxies can be used for anonymizing purposes.

Reconnaissance

Reconnaissance in the context of a hacking attack usually consists of several pre-test phases that are performed prior to the actual attack. The purpose of these pre-tests is to gather as much information about the target computer host, network, or website and its owners and administrating technicians as possible. During the reconnaissance phase, the hacker attempts to gather initial information, determine the network range, identify active hosts and clients, discover active ports and access points, fingerprint the operating systems in use, uncover the active services on ports, and combine all gathered intelligence into a map of the network.

Resource Mismatch

Resource mismatches are one of the most common Denial of Service attacks. They utilize the circumstance that some connections use significant more resources on one side of the connection than on the other. An attacker can exploit such a connection to effectively shut down the target host.

Root shell/kits

On UNIX systems, only the “root” user, the equivalent to a Windows “Administrator,” has complete control over the machine. Several root shell or root kit exploits exist that attempt to obtain a shell prompt with root privileges so as to allow the attacker to enter and execute any command on the target system.

RPC

Remote Procedure Calls are application-to-application network requests designed to execute commands on remote host computers.

RPC port/end-point dump

RPC port/end-point dump scans typically supplement port scans by listing all RPC (Remote Procedure Calls) services running on a system.

Session Hijacking

The term session hijacking refers to the exploitation of a valid computer session to gain unauthorized access to information or services on a computer system. The attacker commandeers a TCP session from a legitimate user after this user has achieved authentication, thereby removing the need for the attacker to authenticate himself.

Shoulder Surfing

A slang word used among hackers to describe an attack method in which the attacker simply monitors the moment the victim enters passwords or other sensitive information on their keyboard.

Social Engineering

The term social engineering encompasses all attempts of attackers to establish and subvert trust relationships with their victims or to predict the behavior of their victims. Once such a relationship is established, the attacker tricks the victim into revealing information or performing an action, such as a password reset, for example, that can then be used in the attack. A subcategory of social engineering methods are so-called reversed social engineering methods, in which attackers

use their expertise to induce their victims to reveal sensitive information when seeking their help and advice.

Source Routing

Source routing denotes a technique that allows a sender of a data packet to specify the route this packet takes trough a network. Source routing can be used in hacking attacks to reach otherwise unreachable targets through intermediate computers that are connected to the target.

Spoofing

Spoofing is a method attackers use to pretend they are somebody else. This is accomplished by creating TCP/IP packets using somebody else's IP address as the source IP address.

TCP/IP

Stands for "Transmission Control Protocol / Internet Protocol" and summarizes a collection of Internet communication protocols between computers that together form the basis for most communications on the Internet.

TOR

Tor (The Onion Router) is a free software implementation of so-called second-generation onion routing. Tor is a system that is similar to I2P in that it enables its users to communicate anonymously on the Internet.

Tunnel

Methods used by hackers to circumvent firewalls and evade intrusion detection systems.

UDP

Or “User Datagram Protocol,” denotes a connectionless information transport protocol that offers a limited amount of services when information is exchanged over the Internet Protocol (IP). It is a faster alternative to the TCP protocol. It does not guarantee delivery or provide sequencing of packets, but is favored for time-sensitive data such as video or audio streams.

URL

URL, or Uniform Resource Locator, is an address that can uniquely specify any Internet resource or file. It consists of the protocol, the domain, and the name of the file.

Versatile Scanning Tools

Versatile scanning tools are software tools that combine a variety of different scanning utilities in one application. A large number of free and commercial scanning tools are available today. As is the case with many other hacking tools, many of these applications are also used for legitimate purposes by system administrators to verify the configurations of hosts in their networks. Versatile scanning tools appeal to attackers because they conveniently combine several of the mapping and scanning functions mentioned earlier. One of the most popular versatile scanning tools is Nmap, a software application that is more than a simple scanner. Nmap allows scanning for RPC (remote procedure calls) services on a target machine, sending decoy scans with fake source addresses, sending scans with different timing options to avoid detection, and identifying a computer’s operating system via fingerprinting, to name but a few functions. Versatile scanning

tools are among the essential hacker tools and are used by hackers of all skill levels.

Vulnerability Scanning

Vulnerability scanning denotes the act of searching for and mapping systems for weaknesses in an application, computer, or network. This search is typically performed by automated vulnerability scanners that combine many functions, such as active network scanning functions and vulnerability scanning functions, in one application. Vulnerability scanners evaluate several types of vulnerabilities including general system weaknesses such as faulty operating system code, faulty application code, or faulty configurations.

War Driving

War driving is the act of driving through an area in a moving vehicle with a WiFi-equipped computer to detect wireless networks that permit the attacker to access the Internet anonymously.

Wetware

A slang word commonly used among hackers and computer experts to signify all methods of programming a brain, as opposed to software. It denotes all social engineering methods.

Whois

Another method for finding out general information about networks, hosts, and their owners are whois requests. Whois is both a searchable public database system of domain names and their registrars and a query utility that provides detailed ownership information about the domain name holders. The whois data-

base system contains information on how to contact the registrar and the technical administrators as well as information on the domain name servers, the registration and expiration date, and the dates the domain was updated. The system was originally developed as a method for system and network administrators to research contact information of other administrators, ISPs, and certified computer incident response teams, and to determine the availability of domain names. Law enforcement agencies also commonly utilize whois queries to lookup domain owners in their combat against online copyright infringements, racial discrimination, hatred, violence, and child pornography. Undoubtedly, the whois system has many positive uses that contribute to a higher user confidence in the Internet as a reliable and efficient communication medium, but it can also be abused to gather intelligence for hacking attacks, especially for attacks on websites. The whois system is not restricted to network administrators, but allows everybody to place queries, regardless of their motivations or intentions. In recent years, the unrestricted access to the whois system has led to increasing abuses by email spammers, who use the system to acquire email addresses for their spam databases. This development that has caused many web site hosts to “lock” their domains in order to prevent spammers from accessing their email addresses, thereby rendering the system less useful than it used to be.

LIST OF REFERENCES

Adam, A. E. (2004). Hacking into Hacking: Gender and the Hacker Phenomenon. *Computers and Society, 32*(7), 3-18

Aguila, N. (2008). The Fifteen Greatest Hacking Exploits: The Birth Of Hacking. Retrieved March 16, 2008, from http://www.tomshardware.com/2008/03/14/the_fifteen_greatest_hacking_exploits/index.html

Akers, R. L. (1990). Rational Choice, Deterrence, and Social Learning Theory in Criminology: The Path Not Taken. *The Journal of Criminal Law & Criminology, 81*(3), 653-676

Akers, R. L., & Sellers, C. S. (2004). *Criminological Theories: Introduction, Evaluation, and Application* (4 ed.). Los Angeles: Roxbury.

Alaganandam, H., Mittal, P., Singh, A., & Fleizach, C. (2005). Cybercriminal Activity. Retrieved February 5, 2008, from http://www.cs.ucsd.edu/~cfleizac/WhiteTeam-CyberCrime.pdf

Alexander, S. (2005). Cyber hackers' motives shift to money. Retrieved May 20, 2008, from http://www.detnews.com/2005/technology/0509/20/A04-320608.htm

Allan, G. J. B. (1976). Ordinal-scaled variables and multivariate analysis: comment on Hawkes. *American Journal of Sociology, 81*(6), 1498-15000

Bachmann, M. (2008). Book Review: Clifford, R. D. (2006). Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime. *International Criminal Justice Review, 18*(2). DOI 10.1177/1057567708319404

Badham, J. (Writer) (1983). War Games. In H. Schneider (Producer). USA: MGM/UA Entertainment.

Beccaria, C. (1764). *Of Crimes and Punishments* (D. Young, Trans.). Indianapolis, Ind: Hackett.

Bednarz, A. (2004). Profiling Cybercriminals: A Promising but Immature Science. Retrieved May 03, 2008, from http://www.networkworld.com/supp/2004/cybercrime/112904profile.html

Bement, A. L., Ward, W. E., Carlson, L. T., Frase, M. J., & Fecso, R. S. (2004). *Women, Minorities, and Persons with Disabilities in Science and Engineering*. Arlington, VA: National Science Foundation, Division of Science Resources Statistics, Document Number 04317)

Bentham, J. (1789). *An Introduction to the Principles of Morals and Legislation*. London: T. Payne.

Bequai, A. (1999). Cyber-Crime: the US Experience. *Computers and Security, 18*(1), 16-18

Blake, C. (2000). *Casting the Runes.* Paper presented at the British Computer Society Information Security Specialist Group seminar, London.

Boudreau, M. C., Gefen, D., & Straub, D. W. (2001). Validation in Information Systems Research: A State-of-the-art Assessment. *MIS Quarterly, 11*(1), 1-16

Bouffard, J. A. (2007). Predicting Differences in the Perceived Relevance of Crime's Costs and Benefits in a Test of Rational Choice Theory. *International Journal of Offender Therapy and Comparative Criminology, 51*(4), 461-485

Brenner, S. (2006). Defining Cybercrime: A Review of State and Federal Law. In R. D. Clifford (Ed.), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime* (pp. 13-94). Durham, NC: Carolina Academic Press.

Cacioppo, J. T., & Petty, R. E. (1982). The need for cognition. *Journal of Personality and Social Psychology, 42*(1), 116-131

Cacioppo, J. T., Petty, R. E., Kao, C. F., & Rodriguez, R. (1986). Central and peripheral routes to persuasion: An individual difference perspective. *Journal of Personality and Social Psychology, 51*(5), 1032-1043

Cammell, D. (Writer) (1977). Demon Seed. In H. Jaffe (Producer). USA: United Artists.

Capeller, W. (2001). Not Such a Neat Net: Some Comments on Virtual Criminality. *Social and Legal Studies, 10*, 229-242

Cartwright, T. (1618). A confutation of the Rhemists translation, glosses, and annotations on the New Testament a 1603.

Casey, E. (2004). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (2 ed.). San Diego, CA & London: Academic Press.

Castells, M. (2002). *The internet galaxy: Reflections on the internet, business, and society*. Oxford: Oxford University Press.

Chirillo, J. (2001). *Hack Attacks Revealed: A Complete Reference with Custom Security Hacking Toolkit*. New York, NY: Wiley.

Clarke, R. V. (1992). Introduction. In R. V. Clarke (Ed.), *Situational Crime Prevention: Successful Case Studies*. Albany, NY: Narrow and Heston.

Clarke, R. V. (1997). *Situational Crime Prevention: Successful Case Studies* (2 ed.). Albany, NY: Harrow and Heston.

Clarke, R. V. (2004). New Challenges for Research: Technology, Criminology and Crime Science. In E. U. Savona (Ed.), *Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research* (pp. 97-104). Dordrecht, Netherlands: Springer.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offender's decisions: A framework for research and policy. In T. M. & N. Morris (Eds.), *Crime and Justice* (Vol. 6). Chicago: University of Chicago Press.

Clarke, R. V., & Cornish, D. B. (2001). Rational Choice. In R. Paternoster & R. Bachman (Eds.), *Explaining Criminals and Crime: Essays in Contemporary Criminological Theory*. Los Angeles: Roxbury.

Clarke, R. V., & Felson, M. K. (1993). *Routine Activity and Rational Choice. Advances in Criminological Theory* (Vol. 5). New Brunswick, NJ: Transaction Press.

Clifford, R. D. (2006). Introduction. In R. D. Clifford (Ed.), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime* (2 ed.). Durham, NC: Carolina Academic Press.

Cohen, L. E., & Felson, M. K. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach *American Sociological Review, 44*(4), 588-608

Computer Crime and Intellectual Property Section, C. D. (2002). *Searching and seizing computers and obtaining electronic evidence in criminal investigations*. Retrieved. from http://permanent.access.gpo.gov/websites/usdojgov/www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm#_VA_.

Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. In R. V. Clarke (Ed.), *Crime Prevention Studies* (Vol. 3). Monsey, NY: Criminal Justice Press.

Cornish, D. B., & Clarke, R. V. (1987). Understanding Crime Displacement: An Application of Rational Choice Theory. *Criminology, 25*(4), 933-948

Cornish, D. B., & Clarke, R. V. (1989). Crime specialisation, crime displacement and rational choice theory. In H. Wegener, F. Losel & J. Haisch (Eds.), *Criminal behavior and the justice system: Psychological perspective* (pp. 103-117). New York, NY: Springer.

Cornish, D. B., & Clarke, R. V. (Eds.). (1986). *The Reasoning Criminal*. New York, NY: Springer.

Cornish, D. B., & Smith, M., J. (2003). *Theory for Practice in Situational Crime Prevention* (Vol. 16). Monsey, NY: Criminal Justice Press.

Couper, M. P. (2000). Web Surveys: A Review of Issues and Approaches. *Public Opinion Quarterly, 64*(4), 464-494

Cramer, D. (2003). A cautionary tale of two statistics: Partial correlation and standardized partial regression. *Journal of Psychology, 137*(5), 507-511

Cronenberg, D. (Writer) (1999). eXistenZ. In D. Cronenberg, A. Hamori & R. Lantos (Producer). Canada: Alliance Atlantis.

Curran, K., Morrissey, C., Fagan, C., Murphy, C., O'Donnell, B., Firzpatrick, G., et al. (2005). Monitoring hacker activity with a Honeynet. *International Journal of Network Management, 15*(2), 123-134

D'Arcy, J. P. (2007). *The Misuse of Information Systems: The Impact of Security Countermeasures*. New York, NY: Lfb Scholarly Pub.

Dahlback, O. (1990). Personality and risk-taking. *Personality and Individual Differences, 11*(12), 1235-1242

Damsell, K. (2003). Ethical Hackers' Test for Weakness*. The Globe and Mail,* p. B1,

De Hann, W., & Vos, J. (2003). A crying shame: The over-rationalized conception of man in the rational choice perspective. *Theoretical Criminology, 7*(1), 29-54

Dinello, D. (2005). *Technophobia!: Science Fiction Visions of Posthuman Technology*. Austin, TX: University of Texas Press.

Dowland, P., Furnell, S., Illingworth, H., & Reynolds, P. (1999). Computer Crime and Abuse: A Survey of Public Attitudes and Awareness. *Computers and Security, 18*(8), 715-726

Dulebohn, J. H. (2002). An investigationof the determinants of investment risk behavior in employer-sponsored retirement plans. *Journal of Management 28*(1), 3-26

Earnest, T. L. (2003). *Deterrence Dynamics and Gender: Extending the Deterrence/Rational Choice Model.* Unpublished Dissertation, Mississippi State U, Oxford, MI.

Edgerton, D. (1995). Technophobia then and now. *Nature, 376*(6542), 653-654

Epstein, S. (2003). Cognitive-experiential self-theory of personality. In T. Millon & M. J. Lerner (Eds.), *Comprehensive Handbook of Psychology, Volume 5: Personality and Social Psychology* (Vol. 5, pp. 159-184). Hoboken, NJ: Wiley.

Epstein, S., Pacini, R., Denes-Raj, V., & Heier, H. (1996). Individual differences in intuitive-experiential and analytical-rational thinking styles. *Journal of Personality and Social Psychology, 71*(2), 390-405

Erickson, J. (2008). *Hacking: The Art of Exploitation* (2 ed.). San Francisco, CA: No Starch Press.

Erickson, K., & Howard, P. N. (2007). A Case of Mistaken Identity? News Accounts of Hacker, Consumer, and Organizational Responsibility for Compromised Digital Records. *Journal of Computer-Mediated Communication, 12*(4), 1229-1247

Ericsson, K., & Simon, H. (1980). Verbal Reports as Data. *Psychological Review, 87*(3), 215-251

Ericsson, K., & Simon, H. (1984). *Protocol Analysis: Verbal Reports as Data*. Cambridge, MA: The MIT Press.

Felson, M. K. (2000). The routine activity approach as a general social theory. In S. Simpson (Ed.), *Of crime and criminality: The use of theory in everyday life*. Thousand Oaks, CA: Sage.

Festinger, L. (1957). *A theory of cognitive dissonance*. Evanston, IL: Row & Peterson.

Finch, J. (1987). The Vignette Technique in Survey Research. *Sociology, 21*(1), 105-114

Fisher, R. J. (1993). Social desirability bias and the validity of indirect questioning. *Journal of Consumer Research, 20*(2), 303-315

Fiske, S. T., & Taylor, S. E. (1984). *Social cognition* (1 ed.). Reading, MA: Addison-Wesley.

Freaky. (2004). ShmooCon. Retrieved Mai 01, 2008, from http://www.hackwire.com/index.php?action=news&catid=11

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

Gibson, W. (1988). *Mona Lisa Overdrive*. Toronto: Bantam Books, Spectra.

Gomez-Mejia, L. R., & Balkin, D. B. (1989). Effectiveness of individual and aggregate compensation strategies *Industrial Relations, 28*(3), 431-445

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). *Computer Crime and Security Survey*: CSI & FBI

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006). *Computer Crime and Security Survey*: CSI & FBI

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2*(1), 13-20

Gosling, S. D., Vazier, S., Srivastava, S., & John, O. P. (2004). Should we Trust Web-Based Studies? A Comparative Analysis of Six Preconceptions About Internet Questionnaires. *American Psychologist, 59*(2), 93-104

Gottfredson, M., & Hirschi, T. (1990). *A General Theory of Crime*. Palo Alto, CA: Stanford University Press.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social and Legal Studies, 10*(2), 243-249

Grabosky, P. N., & Smith, R. (1998). *Crime in the digital age*. Sydney: Federation Press.

Graham, P. (2004). *Hackers and Painters: Big Ideas from the Computer Age*. Sebastopol, CA: O'Reilly Media.

Grecs. (2008). ShmooCon 2008 Infosec Conference Event. Retrieved April 25, 2008, from http://www.novainfosecportal.com/2008/02/18/shmoocon-2008-infosec-conference-event-saturday/

Groves, R. M., Fowler, F. J., Couper, M. P., Lepkowski, J., M., Singer, E., & Tourangeau, R. (2004). *Survey Methodology*. Hoboken, NJ: Wiley.

Gupta, A. K., & Govindarajan, V. (1984). Business unit strategy, managerial characteristics, and business unit effectiveness at strategy implementation. *Academy of Management Journal, 27*(1), 25-41

Hafner, K., & Lyon, M. (1998). *Where Wizards Stay Up Late: The Origins Of The Internet*. New York, NY: Simon & Schuster.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate Data Analysis*. Englewood Cliffs, NJ: Prentice Hall.

Handley, S. J., Newstead, S., E., & Wright, H. (2000). Rational and Experiential Thinking: A Study of the REI. In R. Riding & S. G. Rayner (Eds.), *International Perspectives on Individual Differences: Cognitive Styles* (Vol. 1). Stamford, CT: Ablex Publishing.

Harrington, S. J. (1996). The Effect of Codes of Ethics. and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. *MIS Quarterly, 20*(3), 257-278

Harvey, D. (1989). *The Condition of Postmodernity*. Oxford: Blackwell.

Hawkes, R. K. (1971). The multivariate analysis of ordinal measures. *American Journal of Sociology, 76*(5), 908-925

Hechter, M., & Kanazawa, S. (1997). Sociological rational choice theory. *Annual Review of Sociology, 23*, 191-214

Heckathorn, D. D. (1997). Respondent-Driven Sampling: A New Approach to the Study of Hidden Populations. *Social Problems, 44*(2), 174-199

Howell, B. A. (2007). Real-World Problems of Virtual Crime. In J. M. Balkin, J. Grimmelmann, E. Katz, N. Kozlovski, S. Wagman & T. Zarsky (Eds.), *Cybercrime: Digital Cops in a Networked Environment*. New York, NY: New York University Press.

Howitt, P. (Writer) (2001). AntiTrust. In D. Hoberman, A. Amritraj, C. O. Erickson & J. Chasman (Producer). USA: Metro-Goldwyn-Mayer (MGM).

Jaishankar, K. (2007). Cyber Criminology: Evolving a Novel Discipline with a New Journal. *International Journal of Cyber Criminology, 1*(1), 1-6

Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 281-283). Upper Saddle River, NJ: Pearson.

Jewkes, Y. (2006). Comment on the book 'Cyber crime and Society by Majid Yar. Retrieved September 09, 2007, from http://www.sagepub.co.uk/booksProdDesc.nav?prodId=Book227351

Johnson, B. (2008). Nato says cyber warfare poses as great a threat as a missile attack. Retrieved May 02, 2008, from http://www.guardian.co.uk/technology/2008/mar/06/hitechcrime.uksecurity

Johnston, P. (2008). Tories want new cybercrime police unit. Retrieved March 07, 2008, from http://www.crime-research.org/news/06.03.2008/3236/

Jordan, T., & Taylor, P. A. (1998). A Sociology of Hackers. *The Sociological Review, 46*(4), 757-780

Joseph, J. (2003). Cyberstalking: An International Perspective. In Y. Jewkes (Ed.), *Dot.cons: Crime, Deviance and Identity on the Internet*. Cullompton: Willan.

Kanellis, P., Kiountouzis, E., Kolokotronis, N., & Martakos, D. (2006). *Digital Crime and Forensic Science in Cyberspace*. Hershey, PA: Idea Group.

Kerlinger, F. N. (1986). *Foundations of Behavioral Research* (3 ed.). New York, NY: Rinehart & Winston.

Kilger, M., Arkin, O., & Stutzman, J. (2004). Profiling. In Honeypotproject (Ed.), *Know your enemy: learning about security threats* (2 ed.). Boston: Addison Wesley.

Kim, J.-O. (1978). Multivariate analysis of ordinal variables revisited. *American Journal of Sociology, 84*(2), 448-456

Kim, J.-O., & Mueller, C. W. (1978). *Introduction to Factor Analysis: What It Is and How To Do It (Quantitative Applications in the Social Sciences)*. Newbury Park, CA: Sage.

Koops, B.-J., & Brenner, S. (2006). Cybercrime Jurisdiction - An Introduction. In B.-J. Koops & S. Brenner (Eds.), *Cybercrime and Jurisdiction* (pp. 1-9). The Hague: TMC Asser Press.

Kovacich, G. (1999). Hackers: Freedom Fighters of the 21st Century. *Computers and Security, 18*(7), 573-576

Koziol, J., Litchfield, D., Aitel, D., Anley, C., Eren, S., Neel, M., et al. (2004). *The Shellcoder's Handbook: Discovering and Exploiting Security Holes* (2 ed.). Indianapolis, IN: Wiley.

Kozlovic, A. K. (2003). Technophobic themes in pre-1990 computer films. *Science as Culture, 12*(3), 341-373

Krone, T. (2005). *Hacking motives*. Canberra: Australian Institute of Criminology

Krosnick, J., & Fabrigar, L. (1997). Designing Rating Scales for Effective Measurement in Surveys. In L. Lyberg, P. Biemer, M. Collins, E. de Leeuw, C. Dippo, N. Schwarz & D. Trewin (Eds.), *Survey Measurement and Process Quality* (pp. 141-164). New York, NY: Wiley.

Kubrick, S. (Writer) (1969). 2001: A Space Odyssey. In S. Kubrick (Producer). UK/USA: Metro-Goldwyn-Mayer (MGM).

Kurzweil, R. (2005). The Law of Accelerating Returns. In C. Teuscher & D. Hofstadter (Eds.), *Alan Turing: Life and Legacy of a Great Thinker*. Berlin: Springer.

Lakhani, K. R., & Wolf, R. G. (2003). *Why Hackers Do What They Do: Understanding Motivation and Effort in Free/Open Source Software Projects*: SSRN.

Landler, M., & Markoff, J. (2007). Digital Fears Emerge After Data Siege in Estonia. *The New York Times*. Retrieved August 25, 2007, from http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=1&ei=5070&en=15ee9940d96714da&ex=1188187200

Lemos, R. (2006). Mass defacement puts Turkey on the map. *SecurityFocus*. Retrieved August 29, 2007, from http://www.securityfocus.com/brief/212

Lenk, K. (1997). The Challenge of Cyberspatial Forms of Human Interaction to Teritorrial Governance and Policing. In B. D. Loader (Ed.), *The Governance of Cyberspace: Politics, Technology and Global Restructuring.* London: Routledge.

Levitt, M. (2007). Worldwide Email Usage 2007–2011 Forecast: Resurgence of Spam Takes Its Toll. Retrieved August 25, 2007, from http://www.idc.com/getdoc.jsp?containerId=206038

Levy, S. (1984). *Hackers: Heroes of the Computer Revolution*. New York: Doubleday.

Leyshon, A., Webb, P., French, S., Thrift, N., & Crewe, L. (2005). On the Reproduction of the Musical Economy after the Internet. *Media, Culture & Society, 27*(2), 177-209

Li, F. (2006). *What is e-business: How the Internet Transforms Organizations*. Malden, MA: Wiley-Blackwell.

Lisberger, S. (Writer) (1982). Tron. In D. Kushner (Producer). USA: Buena Vista Pictures.

Littlewood, A. (2003). Cyberporn and moral panic: an evaluation of press reactions to pornography on the internet. *Library and Information Research, 27*(86), 8-18

Longo, R. (Writer) (1995). Johnny Mnemonic. In S. Ahrenberg, D. Carmody, V. Hamburg & R. Lantos (Producer). USA: Sony Pictures.

MacCrimmon, K. R., & Wehrung, D. A. (1990). Characteristics of risk taking executives. *Management Science, 36*(4), 422-435

Mann, D., & Sutton, M. (1998). NetCrime. More Change in the Organisation of Thieving. *British Journal of Criminology, 38*(2), 210-229

Marshall, L. (2004). The Effects of Piracy upon the Music Industry: A Case Study of Bootlegging. *Media, Culture & Society, 26*(2), 163-181

Matsuo, H., McIntyre, K. P., Taomazic, T., & Katz, B. (2004). The Online Survey: Its Contributions and Potential Problems [Electronic Version]. *ASA Secion on Sur-*

vey Research Methods, *1*, 3998-4000. Retrieved Mai, 01 2008, from http://www2.bc.edu/~mcintykc/files/Jsm2004OnlinePaper.pdf

McClintock, R. (1999). Educating America for the 21st Century: A Strategic Plan for Educational Leadership January 2000 through December 2004 Version 2.1 [Electronic Version], 1-25. Retrieved April 01, 2008, from http://www.ilt.columbia.edu/publications/docs/ILT_Plan_new.pdf

Mitchell, W. (1995). *City of Bits*. Cambridge, MA: MIT Press.

Mitnick, K. D., & Simon, W. L. (2005). *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers*. New York, NY: Wiley.

Mitnick, K. D., Simon, W. L., & Wozniak, S. (2002). *The Art of Deception: Controlling the Human Element of Security*. New York, NY: Wiley.

Morris, R. (1970). Multiple correlation and ordinally scaled data. *Social Forces, 48*(3), 299-311

Naughton, J. (2000). *A Brief History of the Future: The Origins of the Internet*. London: Phoenix.

NCIRC. (2008). NATO opens new centre of excellence on cyber defense. Retrieved May 03, 2008, from http://www.nato.int/docu/update/2008/05-may/e0514a.html

Negroponte, N. (1996). *Being Digital* (First Vintage Books ed.). New York, NY: Random House.

Newman, G. R., & Clarke, R. V. (2003). *Superhighway Robbery: Crime Prevention and E-commerce Crime*. Cullompton: Willan Press.

Newsted, P. R., Chin, W., Ngwenyama, O., & Lee, A. (1996). *Resolved: Surveys have Outlived their Usefulness in IS Research.* Paper presented at the Seventeenth International Conference on Information Systems, Cleveland, OH.

Nosek, B. A., Banaji, M. R., & Greenwald, A. G. (2002). E-Research: Ethics, Security, Design, and Control in Psychological Reseach on the Internet. *Journal of Social Issues, 58*(1), 161-176

Nunnally, J. C. (1978). *Psychometric Theory* (2 ed.). New York, NY: McGraw-Hill.

Nuwere, E., & Chanoff, D. (2003). *Hacker Cracker: A Journey from the Mean Streets of Brooklyn to the Frontiers of Cyberspace*. New York: HarperCollins Publishers.

O'Brian. (1979). The use of Pearson's R with ordinal data. *American Sociological Review, 44*(5), 851-857

Opp, K.-D. (1997). Limited rationality and crime. In G. R. Newman, R. V. Clarke & S. S. Giora (Eds.), *Rational Choice and Situational Crime Prevention: Theoretical Foundations* (pp. 47-63). Dartmouth UK: Ashgate.

Oxford English Dictionary (2008). Oxford: Oxford University Press.

Pacini, R., & Epstein, S. (1999). The relation of rational and experiential processing styles to personality, basic beliefs, and the ratio-bias phenomenon. *Journal of Personality and Social Psychology, 76*(6), 972-987

Painter, C. (2004). Threats to the Net: Trends and Law. In E. U. Savona (Ed.), *Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research*. New York, NY: Springer.

Paternoster, R. (1989). Decisions to Participate in and Desist from Four Types of Common Delinquency: Deterrence and the Rational Choice Perspective. *Law & Society Review, 23*(1), 7-40

Pease, K. (2001). Crime futures and foresight: Challenging criminal behaviour in the information age. In D. S. Wall (Ed.), *Crime and the Internet*. London: Routledge.

Piquero, A. R., & Tibbets, S. G. (2002). *Rational Choice and Criminal Behavior. Recent Research and Future Challenges*. New York, NY & London: Routledge.

Porter, S. R., & Whitcomb, M. E. (2003). The Impact of Contact Type on Web Survey Response Rates. *Public Opinion Quarterly, 67*(4), 579-588

Reips, U. D. (2002). Standards for Internet-Based Experimenting. *Experimental Psychology, 49*(4), 243-256

Richtel, M., & Tedeschi, B. (2007). Online Sales Lose Steam. *The New York Times*. Retrieved September 09, 2007, from http://www.nytimes.com/2007/06/17/technology/17ecom.html?ex=1339732800&en=60dbe8c0ab8fec6f&ei=5088

Schell, B. H., Dodge, J. L., & Moutsatsos, S. (2002). *The Hacking of America: Who's Doing It, Why, and How*. New York, NY: Quorum.

Schell, B. H., & Martin, C. (2004). *Cybercrime: A Reference Handbook*. Santa Barbara, CA: ABC-CLIO.

Schlegel, K., & Cohen, C. (2007). The Impact of Technology on Criminality. In J. M. Byrne & D. J. Rebovich (Eds.), *The New Technology of Crime, Law and Social Control* (pp. 23-49). Monsey, NY: Criminal Justice Press.

Schnell, R., Hill, P. B., & Esser, E. (1999). *Methoden der Empirischen Sozialforschung* (6 ed.). Muenchen: Oldenbourg.

Schrutzki, R. (1989). Die Hacker Ethik. In *Das Chaos Computer Buch* (pp. 166-180). Hamburg: Rowohlt.

Shelley, M. W. (1995). Frankenstein. In P. J. Hunter (Ed.), *Frankenstein* (Norton Critical Editions ed.). New York, NY, London: W. W. Norton.

Shields, R. (Ed.). (1996). *Cultures of the Internet: Virtual Spaces, Real Histories, Living Bodies*. London: Sage.

Shinder, D. L., & Tittel, E. (2002). *Scene of the Cybercrime: Computer Forensics Handbook*. Rockland, MA: Syngress Publishing.

Simon, L. (2004). *Dark Light: Electricity and Anxiety from the Telegraph to the X-Ray*. Orlando, FL: Harcourt.

Slovic, P. (1972). Information processing, situation specificity and the generality of risk-taking behavior. *Journal of Personality and Social Psychology, 22*(2), 128-134

Snyder, F. (2001). Sites of Criminality and Sites of Governance. *Social and Legal Studies, 10*, 251-256

Softley, I. (Writer) (1995). Hackers: Boot Up or Shut Up! In M. Peyser (Producer). USA: Metro-Goldwyn-Mayer (MGM).

Sommer, R., & Sommer, B. (2002). *A practical guide to behavioral research: Tools and techniques* (5 ed.). New York: Oxford University Press.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 255-276

Sykes, G., & Matza, D. (1957). Techniques of neutralization: a theory of delinquency. *American Sociological Review, 22*, 664-670

Taylor, P. A. (1999). *Hackers: Crime in the digital sublime*. London and New York, NY: Routledge.

Taylor, P. A. (2000). Hackers - Cyberpunks or Microserfs. In D. Thomas & B. Loader (Eds.), *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. London: Routledge.

Taylor, P. A. (2004). Hacktivism - Resistance is Fertile? In C. Sumner (Ed.), *The Blackwell Companion to Criminology*. Oxford: Blackwell.

Thomas, D. (2002). *Hacker Culture*. Minneapolis, MN: University of Minnesota Press.

Thomas, D. (2002). Notes from the Underground: Hackers as Watchdogs of Industry. *Online Journalism Review*. Retrieved March 2, 2008, from www.ojr.org/ojr/business/1017969515.php

Thomas, D., & Loader, B. D. (2000). Introduction - Cybercrime: law enforcement, security and surveillance in the information age. In D. Thomas & B. Loader (Eds.), *Cybercrime: law enforcement, security and surveillance in the information age*. London: Routledge.

Thompson, B. (2004). *Exploratory and Confirmatory Factor Analysis: Understanding Concepts and Applications*. Washington, DC: American Psychological Association.

Tourney, C. P. (1992). The Moral Character of Mad Scientists: A Cultural Critique of Science. *Science, Technology, & Human Values, 17*(4), 8

Trochim, W. M. K. (2002). *The research methods knowledge base* (2 ed.). Cincinnati, OH: Atomic Dog Publishing.

Tudor, A. (1989). *Monsters and Mad Scientists: A Cultural History of the Horror Film*. Oxford: Blackwell.

Turkle, S. (1995). *Life on the Screen: Identity in the Age of the Internet*. New York, NY: Simon and Schuster.

Turner, D., Fossi, M., Johnson, E., Mack, T., Blackbird, J., Entwisle, S., et al. (2008). Symantec Global Internet Security Threat Report: Trends for July - December 07. Retrieved May 08, 2008, from http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf

Twist, J. (2003). Cracking the hacker underground. Retrieved February 27, 2008, from http://news.bbc.co.uk/1/low/technology/3246375.stm

Computer Fraud and Abuse Act, 1030 C.F.R. (1986).

Vallee, J. (2003). *The Heart of the Internet: An Insider's View of the Origin and Promise of the On-Line Revolution*. Charlottesville, VA: Hampton Roads.

Voiskounsky, A., Babeva, J., & Smyslova, O. (2000). Attitudes towards Computer Hacking in Russia. In D. Thomas & B. Loader (Eds.), *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. London: Routledge.

Wall, D. S. (2001). Cybercrimes and the Internet. In D. S. Wall (Ed.), *Crime and the Internet*. London: Routledge.

Warner, J. (2007). U.S. Online Banking Population Grew 9.5% In 2006. *Online Media Daily*. Retrieved September 20, 2007, from

http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticle&art_aid=59070

Webster, J. (1996). *Shaping women's work: Gender, employment and information technology*. London: Longmans.

Wright, B. R. E., Caspi, A., Moffit, T. E., & Paternoster, R. (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), 180-213

Yar, M. (2005a). Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal, 44*(4), 378-399

Yar, M. (2005b). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology, 2*(4), 407-427

Yar, M. (2006). *Cybercrime and Society*. London: Sage.

Zarrett, N. R., & Malanchuk, O. (2005). Who's computing? Gender and race differences in young adults' decisions to pursue an information technology career. *New Directions for Child and Adolescent Development, 2005*(110), 65-84

Zone-H. (2007). Attackers Top List. *Digital Attacks Archive*. Retrieved September 09, 2007, from http://www.zone-h.org/component/option,com_topatt/Itemid,48/