University of Missouri, St. Louis
IRL @ UMSL

Dissertations   UMSL Graduate Works

11-22-2005

Hacks, Cracks, and Crime: An Examination of the Subculture and Social Organization of Computer Hackers

Thomas Jeffrey Holt
University of Missouri-St. Louis, tjholt@email.uncc.edu

Follow this and additional works at: https://irl.umsl.edu/dissertation

Part of the Criminology and Criminal Justice Commons

Hacks, Cracks, and Crime: An Examination of the Subculture and Social

Organization of Computer Hackers

by

THOMAS J. HOLT
M.A., Criminology and Criminal Justice, University of Missouri- St. Louis, 2003
B.A., Criminology and Criminal Justice, University of Missouri- St. Louis, 2000

A DISSERTATION

Submitted to the Graduate School of the

UNIVERSITY OF MISSOURI- ST. LOUIS

In partial Fulfillment of the Requirements for the Degree

DOCTOR OF PHILOSOPHY

in

Criminology and Criminal Justice

August, 2005

<u>Advisory Committee</u>

Jody Miller, Ph. D.
Chairperson
Scott H. Decker, Ph. D.
G. David Curry, Ph. D.
Vicki Sauter, Ph. D.

ABSTRACT

This dissertation examines both the subculture and social organization practices of computer hackers. The concept of normative orders (Herbert, 1998: 347) is used to explore hacker subculture in different contexts. To assess hacker social organization, I use Best and Luckenbill's (1994) framework of organizational sophistication as well as measures from Decker et al. (1998). The relationships between subculture, social organization, and behavior are explored as well. I collected three qualitative data sets to explore these issues, including posts from six on-line hacker discussion forums, in-depth interviews with active hackers, and field observations at the Defcon 12 hacker convention. These data were triangulated and used to investigate the research questions.

The findings suggest the social world of hackers is shaped by five normative orders: technology, knowledge, commitment, categorization, and law. These orders are interrelated, and overwhelmingly influenced by technology. Furthermore, hackers tend to perform hacks alone, but have relatively loose social networks that are used to share information and introduce subcultural norms to new hackers. These networks are couched in a larger hacker community that provided access to a variety of resources and materials. Finally, this analysis demonstrates the dynamic relationships between subculture, social organization, and behavior. I found that subculture and social organization structure the nature of deviant relationships, norms, and behavior. At the same time, the nature of deviant acts appears to influence social organization and subculture. I also discuss the implications for research on computer hackers and crime generally.

DEDICATION

Many people deserve recognition for their assistance in the completion of this dissertation. To begin, I greatly appreciate Jody Miller for her tireless efforts as chair of my dissertation committee. Her advice on both research and writing was indispensable in shaping this work. The same can be said for Scott Decker, especially with regard to policy and law enforcement applications of this study. Many thanks go to Dave Curry and Vicki Sauter for their insights and aid throughout the course of this study. Furthermore, I am grateful for the training and education provided by the faculty of the Department of Criminology and Criminal Justice at UMSL. Their efforts have molded my abilities as a researcher and academic.

I must also thank the individual interviewees who participated in this study. Without their information and experiences, I would never have been able to understand hacking and hacker subculture. Mack Diesel requires special recognition for his assistance as a key informant. This research could not have been completed without his advice and insight. Vicki Sauter should also be thanked for her efforts in identifying participants.

Justin Shacklette, Demond Powell, Kevin Fowler, and my fraternity brothers must also be thanked for their constant support and willingness to drag me out for a night of pro wrestling and movies. The constant "nerd" comments have always brought me great comfort. I must also express my gratitude to Brad Brick, Kim Martin, and Rob Fornango for their ability to listen and humor me when things became tough. In addition, Gus and Ellie Holt should be recognized for their help over the years.

Bob and Marilee Ingoldsby also deserve thanks for their help and support throughout my graduate studies. I also greatly appreciate my sister and brother-in-law Melissa and Mike Haley for the love and support they have shown. Their willingness to listen, help, and laugh throughout this time has been invaluable. I must also thank my parents, Bruce and Ginger Holt, who have given nothing but love and concern over the years. You have always provided great support and been there when I needed you.

I must also express my gratitude to my wife Melissa for all that she has done for me. She has been my rock and anchor throughout my time as a graduate student. Despite various difficulties and bumps in the road, her love and care have been unwavering. I cannot put into words how grateful I am to have you as my wife, and cannot imagine life without you. I only hope to show you the same love and joy that you give me every day.

Finally, my grandfather Jeff Layton deserves special recognition for his support throughout my life. He has been a benefactor who has helped me whether as a young boy or newlywed. Regardless of what changes have occurred, he has always been there to help in any way. Without his assistance, my life would not be the same. I dedicate this work to my grandfather, wife, and family who made all of this possible. I do not have the words to fully express what you have done for me; I can only say thank you.

CONTENTS

ILLUSTRATIONS

TABLES

CHAPTER ONE: INTRODUCTION

This dissertation examines both the subculture and social organization practices of computer hackers. These concepts are interrelated, representing social aspects of crime (Warr, 2002; Best and Luckenbill, 1994). They also impact law enforcement and policy makers who must adjust responses to crime based on the organization of deviants (Best and Luckenbill, 1994: 13). The goals of this dissertation are threefold. First I identify the normative orders of hacker subculture in different contexts (Herbert, 1998: 347). Second, I examine hackers' level of organization measured through hacker complexity of divisions of labor, coordination of roles, and purposiveness of associations (Best and Luckenbill, 1994: 12; Decker et al., 1998). Finally, I consider the conceptual linkages between the subculture, social organization, and behavior and their influences on one another. To explore these issues, I use a variety of data including on-line hacker discussion forums, in-depth interviews with active hackers, and field observations.[1] As a whole, these analyses will increase the academic understanding of hackers and the social aspects of crime generally, with specific benefits to law enforcement and policy makers as well.

The social aspects of crime are central to criminology because they address the nature of criminal behavior, associations, and organization. This is especially needed for hackers as they represent an increasingly significant yet misunderstood problem for computer users across the globe (Furnell, 2002). Specifically, computer hackers are individuals with a profound interest in computers and technology that have used their knowledge to access computer systems (Schell et al., 2002). Though the hacker is just

---

[1] The on-line forums used in this data set are created and run for hackers by hackers. They allow hackers to communicate and exchange information on different issues.

one type of computer criminal, they are by far the most easily recognized offenders[2] (Best and Luckenbill, 1994). Many in the general public identify hackers as a primary threat to computer users (Furnell, 2002: 28; UK National Computing Centre, 1994). This may be due to the significant media attention given to dramatic computer crimes attributed to hackers (Furnell, 2002: 29).

As a result, businesses, law enforcement agencies, governments, and computer users world-wide have become more concerned with hacker-related computer crime (Furnell, 2002). In fact, the risks of computer crime victimization have increased around the globe (Holt, 2003), and numerous attempts have been made to deal with the problem. Individual nations and international bodies have recently created legislation to combat these crimes (Norman, 2001). Businesses have also taken action against computer criminals, especially hackers. For example, Microsoft recently announced they would offer monetary rewards for information leading to the capture of computer hackers and virus writers (Lemos, 2003). Researchers from a variety of fields, including criminology (Loper, 2000), computer science (Furnell, 2002), psychology (Woo, 2003), and military sciences (Kleen, 2001), have developed a diverse literature on hackers.

Despite such efforts to understand computer crime, several issues require clarification, from the undercounting of computer crime (Holt, 2003) to difficulties enforcing laws against these offenses (Wall, 2001). Researchers do not yet have a complete understanding of computer criminals, particularly hackers. Still, examinations

---

[2] There are many types of computer criminals, including "phreaks" who have great interest in phone systems and hack into them for different reasons (Thomas and Loader, 2000: 6-7). Another is the malware writer who creates and in some cases distributes computer "viruses, worms, and Trojan Horses" (Furnell, 2002: 44). "Deviants" have also been suggested based on their sharing or posting child pornography on-line (Thomas and Loader, 2000: 7). These are just a few of the criminal types that have been identified (see Thomas and Loader, 2000: 6-7 for further discussion).

of the subculture and social organization of hackers have increased our knowledge of the social aspects of hacking. Specifically, subcultural studies have successfully identified values, norms, and beliefs of hackers (Meyer, 1989; Jordan and Taylor, 1998; Taylor, 1999; Loper, 2000; Thomas, 2002; Wysocki, 2003). In turn, this has illustrated how and why involvement in the subculture influences hackers' behavior. However, the elements that compose this subculture may change over time, or may appear to differ due to the sampling and methods used (see Short, 1968). As such, it is necessary to continue the examination of hacker subculture to expand our knowledge of its value systems and impact on individuals and their behavior.

Research on the social organization of hackers has improved our understanding of how these individual operate within the subculture on their own and in group contexts (Best and Luckenbill, 1994). This knowledge has also assisted law enforcement in responding to hackers and hacker groups (Best and Luckenbill, 1994). A groundbreaking study by Meyer (1989) found that hackers were colleagues and in some cases peers, but their offenses and culture did not promote any organizational sophistication. Thus, they did not form any real lasting formal organizations. Unfortunately there have been no attempts to replicate Meyer's study in the intervening 15 years. Given the vast changes in computer technology and use during this period, it is necessary to build from Meyer's (1989) previous research and consider the current state of hacker social organization.

Through this dissertation I will expand on previous research to examine hacker subculture, as well as the social organization of hackers. This study also considers the interrelations between social organization, subculture, and behavior, which researchers rarely examine. To accomplish this, I use qualitative research methods to collect and

analyze multiple data sources. This includes posts to six on-line computer hacker forums, in depth interviews with computer hackers, and field observations from the DefCon hacker convention in Las Vegas, Nevada. These data are triangulated (Miles and Huberman, 1984) and used to investigate both the key elements of hacker subculture and their current social organization practices.

I utilize inductive analyses of multiple qualitative data sets to address the research questions. This strategy allows the findings to develop from the data. Such methods provide a useful way to achieve the goals of this research, including understanding the values, beliefs, and rationalizations that compose the normative orders of hacker subculture in different contexts. In addition, I will ascertain the current level of hacker social organization based on the complexity of divisions of labor, coordination of roles, and purposiveness of hacker associations (Best and Luckenbill, 1994). With these analyses, I hope to improve academic knowledge of the social aspects of hackers, and in doing so, contribute to the study of social aspects of crime generally.

The remainder of the chapter reviews the definitional issues and classifications of hackers. I also provide a brief history of hackers, highlighting the social and technological developments that have shaped the image of hackers. Then I will present the research literature on hacker subculture and its social organization. Previous studies and their findings guide this research and its methodology. I conclude with an outline of the dissertation.

A HACKER PRIMER

DEFINING HACKERS

One of the more difficult issues faced by researchers interested in hackers is in defining these individuals and their behavior. There are now several terms attached to the hacker, as well as different sub-classifications (see Furnell, 2002). For the purposes of this dissertation, I define a hacker as any individual with a profound interest in computers and technology that has used this knowledge to access computer systems with or without authorization from the system owners. Authorization is critical because individuals who hack without it are committing a crime. Those with permission, however, are not technically breaking the law. Thus, my definition recognizes both criminal and non-criminal hackers. Individuals who perform hacks or related behaviors are also included in my research definition. Specifically, I include anyone who has engaged in phone phreaking, software cracking, malware writing or programming, wardriving, or posting in hacker web forums.

Each of these activities are related to hacking and may be performed by hackers. Phone phreaking involves hacking into or utilizing telephone networks for illegal activities. While some have suggested this behavior constitutes a separate category of computer crime (see Thomas and Loader, 2000), hackers often break into telephone systems to assist in accomplishing hacks (Slattalla and Quittner, 1995). The same can be said for software cracking, which involves overcoming copy protection devices in software to copy and distribute them (Furnell, 2002: 44). Likewise, writing or programming malware software such as viruses and trojan horse programs is a growing computer crime problem and has been connected to hackers (Furnell, 2002: 44).

Wardriving, or traveling with equipment to identify wireless networks and exploit or attack them is also an increasingly common behavior among hackers (Webopedia, 2003).

I also include persons who post in hacker web forums, as these are frequented by both aspiring and experienced hackers. Web forums are one of the primary places a novice hacker can visit to connect with others and ask questions (see Landreth, 1985; Meyer, 1989). Thus, these forums provide a way to bring individuals into hacker subculture. Observing the enculturation process of hackers is critical for this research, and is the reason I include people who post in these forums in the research definition.

While such an expansive definition may seem unnecessary, the hacker population represents individuals with a broad spectrum of personal motivations, skills, and activities (see Furnell, 2002 for discussion). For example, one of the more inclusive definitions from outside the hacking world is from the Jargon File. This text document, which defines and translates hacker slang, provides eight different definitions for a hacker, ranging from the 1960s concept of a skilled computer user, to contemporary applications of someone who maliciously attempts to "discover sensitive information by poking around" (Jargon File; Furnell, 2002: 42). The emphasis on gaining unauthorized access to computer systems is key to the notion of hackers that has been promulgated in the popular media over the last decade (Thomas and Loader, 2000). However, researchers suggest there is no real consensus as to what constitutes a hacker (see Loper, 2000; Voiskounsky et al., 2000).

This is reflected as well in debates between hackers over definitions (Jordan and Taylor, 1998; Loper, 2000), though many hackers associate with the spectrum of behavior identified in the Jargon File. Hackers often distinguish themselves from each

other using the terms white-hat, black-hat, or grey hat (see Furnell, 2002; Thomas, 2002).

White hats are generally "ethical" hackers who work to find errors in computer systems

and programs, and may use unauthorized entry into systems to benefit the computer

security industry (Furnell, 2002: 43). Conversely, black hats seek these same errors to

gain access to information or harm a system, often making them the focus of media and

law enforcement attention (Furnell, 2002: 43). Grey hat hackers fall somewhere between

these two camps, having unclear or changing motives depending upon the specific

situation (Furnell, 2002: 43). Each of these classifications are typically reserved for

those in the upper echelons of hacking with demonstrable skill and technical knowledge.

There are also terms attached to those with much less skill or different behaviors,

including the "cracker" and "script kiddie" (Furnell, 2002: 42-44). The "cracker" hacks

into systems to destroy or harm them. Many hackers could be labeled as crackers, and

their actions are quite similar to those of black hats. However, true hackers consider

these individuals to be "a lower form of life" because of their destructive behavior

(Furnell, 2002: 42). A cracker may however have more skill and ability than the "script

kiddie" (Furnell, 2002: 44). These individuals have relatively limited hacking skills and

use programs or scripts written by other hackers to cause damage and mischief on-line.

Script kiddies generally attack systems without fully understanding how both the

program they use and the system they target operate. Usually they are people new to the

hacking scene that garner little respect from older, more experienced hackers who may

also call them "lamers," "lusers," and "wannabees" (Furnell, 2002: 44). Script kiddies

may also be responsible for a large number of poorly planned or unsophisticated hacks,

which may account for why they are poorly regarded by other hackers (Schell et al., 2002: 5).

There are even further classifications within the hacker community. The term "cyber terrorist" refers to individuals who use hacking techniques to attack networks, systems, or data under the name of a particular social or political agenda (Furnell, 2002: 44). "Hactivists" are those who break into computer systems to promote an activist agenda, often defacing web sites to express an opinion (Furnell, 2002: 44). This is by no means an exhaustive list of the different labels applied to those in the hacking community, however it demonstrates the remarkable variation complicating research on these individuals. As a result, individuals who demonstrate these disparate behaviors and attitudes are included in the definition I use for "hacker."

A BRIEF HISTORY OF HACKERS

To better understand and appreciate how these different definitions for hackers have developed, they must be considered in an appropriate social context. Hackers have existed since computing was in its infancy and have changed with social movements and improvements in computer technology. In the late 1950s, the term hacker was coined to refer to computer software and hardware experts at MIT, Cornell, and Harvard who developed elegant solutions to problems that occurred with then slow-functioning mainframes (Levy, 1984). At the time computing and programming took place primarily in university settings with very large mainframe computers housed away from users in sealed, climate-controlled rooms. Users and programmers had to wait long periods of time while computers processed information. Hackers helped speed up the process by developing techniques to alter existing programs by removing lines of code. This

advanced the technology of computing and led programmers to be called hackers and their activities hacks, as a sign of respect for their skills (Furnell, 2002).

This conception of the hacker continued into the 1960s when the computer moved from universities into military applications (Thomas, 2002). However, a shift occurred as a consequence of the turbulent social climate of the 1960s, as well as the Vietnam War. Military applications angered many programmers of the day, despite their work being funded largely by the military and federal government (Thomas, 2002).

Programmers' beliefs began to take shape in a series of ideals forming part of the core of hacker culture. Specifically, "hackers" of this period believed information should be free to all to understand how things work and can be improved (Thomas, 2002: 15). This notion formed the centerpiece of a series of related ideas called the Hacker Ethic (Levy, 1984), briefly summarized as follows (Furnell, 2002: 64; Levy, 1984):

1. Access to computers- and anything which might teach you something about the way the world works- should be unlimited and total.

2. All information should be free.

3. Mistrust authority- promote decentralization.

4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.

5. You can create art and beauty on a computer.

6. Computers can change your life for the better.

This ethic guided the actions of hackers and formed the roots of the present hacker culture (Levy, 1984). At this point, hackers were viewed as skilled computer users. However, a subtle shift began to occur in the 1970s with the development of

"phone phreaking" (Landreth, 1984). This involved tampering with phone technology to understand and, in some cases, control telephone systems (Landreth, 1984). Phreaking allowed individuals to make free calls to anyone in the world by controlling telephone system switches.

This became notorious because of a man named Cap'n Crunch (John Draper), who blew a giveaway whistle found in a box of cereal into his phone receiver (Landreth, 1984: 31). The whistle created the perfect 2600 megahertz tone that, at the time, was used to connect an individual to long distance lines. This simple toy opened a new area of technology for individuals to explore and exploit, particularly those interested in computers and hacking. Also during the late 1970s, the first personal computer bulletin board system (BBS) was created (Thomas, 2002). A BBS is essentially an on-line system which allowed individuals to post comments and information. In turn, others could read and respond to those posts (Meyer, 1989: 14). Thus hackers could come together on-line to share and discuss information and interact socially (Thomas, 2002). However, the real impact of these developments would be felt during the next decade.

During the 1980s a new breed of computer user challenged the hacker ethic. Because of changes in technology and society, more individuals had access to computer technology. Specifically, IBM's new stand alone "personal computer" brought computer technology to a new generation and into more homes than ever. Modem technology, which connects computers to other computers and networks via telephone lines, also improved. This equipment allowed individuals with personal computers to connect to other dedicated computer users. As a result, the exploration of computer networks was now possible for individuals outside of university and business settings (Furnell, 2002).

Modems also increased the number of individuals on-line and changed the shape of the

computer underground (Furnell, 2002). Finally, the 1983 film *War Games* introduced the

general public to the rather unexplored world of computer hacking. The film suggested

young males with computers could break into any computer system in the world and

wreak havoc without anyone ever knowing. This film and its message had a significant

influence on a new generation of computer users (Furnell, 2002; Thomas, 2002).

With more computer users logged on in the 1980s, BBSs became even more

important for hackers. Budding hackers shared detailed information about systems they

explored and bragged about their exploits (Landreth, 1984). The boards also allowed

hackers to form groups with private networks and create password protected boards to

keep out the uninitiated and maintain privacy (Landreth, 1984). Some of these groups,

such as the 414's, Masters of Disaster, and Legion of Doom, broke into especially

sensitive computer systems. In doing so, they brought law enforcement agencies to bear

on the activities of hackers across the United States (Sterling, 1992). Increasingly risky

and law breaking hacks perpetrated by these groups tested the limits of the hacker ethic

and drew media attention to the exploits of criminal hackers.

Hacker culture became further divided during the 1980s with the posting of a

brief text called "The Conscience of a Hacker," also referred to as "The Hacker

Manifesto." A member of the notorious hacker group Legion of Doom, named "The

Mentor," wrote this text in 1986. The author railed against adults, law enforcement, and

schools (Furnell, 2002: 59). He also suggested hackers explore and seek knowledge even

if that means breaking into or gaining access to otherwise protect computer systems.

However, the author stated this should not make hackers criminals. The Mentor also

encouraged hackers to use telephone systems without paying for the service because they are "run by profiteering gluttons" (Furnell, 2002: 59; The Mentor, 1986). This unapologetic post derided the traditional hacker definition espoused in the 1960s, as well as the "Hacker Ethic." The document provided support for the increasingly criminal nature of hacker activities. The growing literature on cyberspace also reinforced the notion of hackers as digital cowboys or outlaws on the electronic frontier (Gibson, 1983; Barlow, 1990). Thus, the term hacker began to take on a different meaning during the 1980s.

Within a few years the Manifesto became widely read, and computer users without real technical skill became interested in hacking. This caused a rift between hackers with malicious intent and those with an interest in exploring networks without breaking the law or violating privacy. The divide was also fueled by different beliefs, as represented in the Hacker Manifesto (The Mentor, 1986) versus the Hacker Ethic (Levy, 1984). In addition, malicious hackers became the focus of law enforcement during the mid-to-late 1980s. High profile hacking incidents took place, such as the well-documented battle between the LOD and MOD (see Slatalla and Quittner, 1995), and the attacks of Kevin Mitnick (see Shimomura and Markoff, 1996) and Kevin Poulson (see Littman, 1997).

Several high profile arrests were made and hacker groups splintered under government crackdowns such as Operation Sundevil and Crackdown Redux (Sterling, 1992). However, these law enforcement efforts had little deterrent effect on hackers and hacking culture. The development of user friendly computer systems and the growth of the Internet and World Wide Web made the home computer ubiquitous. New users also

became interested in hacking with the release of the film "Hackers" in 1995 (Thomas, 2002). This film's presentation of hackers helped cement the notion that hackers are criminals. The growth of computer culture and further advancements in technology further divided hackers by motivation, affiliation, and activity. Thus, the current hacker culture is rife with different sorts of hackers, each with specific agendas.

LITERATURE REVIEW

SUBCULTURAL THEORIES

The historical context of hacking illustrates the counterculture roots and nature of hacking. This demonstrates why social scientists have used a subcultural perspective to examine hackers. The notion of subculture is an important way for researchers to consider how and why individuals engage in criminal behavior (see Short, 1958; Miller, 1958). Since there is significant debate over what constitutes a subculture (see Agnew, 1995), it may be best to approach the question by determining its main characteristics.

Defined from a broad sociological perspective, a subculture is any group having certain values, norms, traditions, and rituals that set them apart from the dominant culture (Kornblum, 1997; Brake, 1980). This includes an emphasis on performing certain behaviors or developing skill sets, like confidence men learning to grift (Maurer, 1974). Also, subcultural rules or codes of conduct exist that structure how individuals view and interact with different groups (Foster, 1990). A special argot or slang is present, as well as some outward symbols of membership like tattoos or informal uniforms (Simmons, 1985). These all provide ways to measure an individual's reputation, status, and adherence to the subculture.

This framework suggests membership in a subculture influences behavior by providing individuals with beliefs, goals, and values that approve of and justify particular types of activities, including crime (Herbert, 1998). In the case of offender subcultures, the transmission of subcultural knowledge increases the likelihood of involvement in criminal behavior despite potential legal consequences for these actions. Thus, this is an important perspective to explain how the values and ideas espoused by members of a criminal subculture affect the behavior of its members.

Different types of subcultural frameworks have been developed and vary based on assumptions about the members' adherence to conventional norms and values. For example, Cohen (1955) used strain theory to explain the formation and persistence of gangs in the lower classes. Males who could not achieve status through legitimate means in schools felt strained and rebelled against the middle class values imposed on them. They established an alternative subculture allowing them to achieve status through the use of illegitimate means, including property and violent crime. Cohen's framework suggests that this subculture held behaviors and values in direct opposition to the middle class values espoused by groups such as the school. As such, this perspective on subculture assumes an outright rejection of conventional norms and values.

Other frameworks do not require members of a subculture to perfectly adhere to its specific values. For instance, Wolfgang and Ferracuti (1967) suggested a subculture of violence exists wherein individuals place great importance on their honor and use violence to defend it. According to their theory, this subculture does not require individuals to accept or approve of its norms for their behaviors to be influenced.

Anyone may use lethal violence at any time, so all must be willing to respond to this

threat in kind.

A similar argument has been made by Anderson (1999) in *Code of the Streets*.

He suggests a code exists in inner city communities that leads individuals to conform to a

pattern of violent behavior on the streets in response to slights against their honor.

Regardless of one's involvement in street life and its values, many conform to this code

of behavior to navigate through their communities. Thus, a contrasting perspective

indicates subcultures can influence behavior without requiring individuals to adhere to its

values.

Recent research on the subculture of policing has attempted to bridge these two

competing perspectives of enculturation through the concept of "normative orders"

(Herbert, 1998: 347). This is a "set of generalized rules and common practices oriented

around a common value" (Herbert, 1998: 347). An order "provide[s] guidelines and

justifications" for behavior, demonstrating how subcultural membership impacts actions

(Herbert, 1998: 347). This is a dynamic view of culture, recognizing the importance of

cultural values in unconsciously shaping behavior. Specifically, the term "normative

order" is derived from Parsons (1937) who argued social cohesion results from the

consistent acceptance of values across social groups. However, some argue this

perspective makes humans "cultural dopes" with no influence over their behavior (see

Garfinkel, 1967; DiMaggio and Powell, 1991).

Herbert's (1998) concept moves beyond these critiques by acknowledging the

impact of decision-making in shaping and accepting cultural values. For example, the

definition of normative order allows the researcher to consider how rules lead individuals

to reflexively construct and respond to others in social situations (Herbert, 1998: 348). This encompasses formal written rules as well as those developed informally based on the values they uphold. Furthermore, the concept of normative order is flexible enough to identify conflicts occurring in the subculture through contradicting orders (Herbert, 1998: 350). Hence, normative orders recognize that individual behavior is influenced by personal decisions, as well as through adherence to the values of a given subculture. Because of the dynamic view of culture provided by this perspective, I will use normative orders to inductively examine hacker subculture.[3]

PREVIOUS RESEARCH ON HACKER SUBCULTURE

Several researchers suggest that characteristics of a subculture can be found in the hacking community (Meyer, 1989; Jordan and Taylor, 1998; Taylor, 1999; Loper, 2000; Thomas, 2002; but see Wysocki, 2003). There is strong evidence of the presence of a social scene, slang, and value system that defines boundaries between hackers and others (see Meyer, 1989; Jordan and Taylor, 1998; Taylor, 1999; Loper, 2000; Thomas, 2002). These studies are important as they provide a deeper understanding of hacker subculture, highlighting the values and norms that affect the behavior of its members. For example, the act of hacking is illegal under most conditions, yet the skill and ability needed to perform a hack is highly valued among hackers (Thomas, 2002). In addition, many hackers acknowledge their activities are illegal, but legitimize and justify the actions using various rationales (Furnell, 2002). Thus, hackers place emphasis and value on activities directly contradicting the larger culture.

---

[3] Since this is a qualitative study, all normative orders are identified inductively based on the respondents' views on given issues rather than through any pre-existing framework. A detailed discussion on the process of identifying normative orders in this research is provided in Chapter Two.

In addition, hackers have adapted the English language to create a unique slang (see Meyer, 1989). There also appears to be a hacker "scene," composed of "inside jokes, real world meetings (cons) and hacker magazines ('zines)" (Loper, 2000: 66). Understanding this "scene" is part of the enculturation process of hacker subculture, occurring through exchanges with other hackers either in person or on-line (Fiery, 1994: 106-108). Referencing these cultural elements permit individuals to measure their status as a hacker against others (Loper, 2000, Meyer, 1989). Status can also be determined through the great deal of debate over what constitutes a "hacker" as well as motives for hacking, such as curiosity or revenge (Jordan and Taylor, 1998). These debates create boundaries between hackers, as well as the general computer using public, based on knowledge, skill, and status (see Taylor, 1999).

While many elements of hacker subculture have been identified across studies and over time, some features appear in one study but not others. This may be the result of methodology, sampling, or timeframe, but such discrepancies suggest the research literature should be closely analyzed to better understand what significant and lasting features characterize hacker subculture.

One of the most recognized elements of hacker subculture is its relationship to technology (Jordan and Taylor, 1998; Taylor, 1999; Thomas, 2002). Both the hack and hacker could not exist without technology, and an intimate connection between the individual and technology facilitates the ability to hack (Taylor, 1999). To generate such a connection, hackers must develop "an easy, if not all-consuming, relationship" with computer and communications technology and a willingness to explore and apply it in new ways (Jordan and Taylor, 1998: 764).

The more closely an individual is connected to technology, the greater their ability to understand and perform hacks. Those who can perform "true hacks" have a deep comprehension of computers and programming, allowing them to identify and fix security flaws (Thomas, 2002: 44). Conversely, "derivative hacks" involve the use of pre-written scripts or codes to access flaws without actually understanding how the technology works (Thomas, 2002: 43). Less skilled hackers, especially script kiddies, are more likely to perform a "derivative hack" (Furnell, 2002: 44). Hence, the hacker's relationship to technology can generate status: those who complete "true hacks" are revered, and the "derivative hack" user is often reviled (Thomas, 2002: 37).

The importance of technology is also related to the significance of secrecy in hacker subculture (Jordan and Taylor, 1998; Taylor, 1999; Thomas, 2002). Secrecy is important for several reasons. First, it is a motive for hacking in that many hackers abhor keeping certain types of information private (Thomas, 2002: 40). This fuels many attempts by hackers to remove barriers to certain kinds of information, such as government and technological data (Thomas, 2002: 40).

Second, subcultural members place great emphasis on secrecy because hacking is an illegal act (see Taylor, 1999). Hacker activities are kept secret to avoid unwanted attention from various parts of the "establishment," including the criminal justice system (Taylor, 1999: 29). Thus, anonymity is indispensable to the subculture, and is the reason hackers create virtual identities on-line via a screen name or "handle" (Jordan and Taylor, 1998: 765). This protects the hacker's actual identity while engaged in hacking.

However, there is also some ambivalence about secrecy in hacker subculture. Successful hacking creates a desire to brag and share accumulated hacking knowledge

(Jordan and Taylor, 1998). This can help an individual gain status within the hacker community, but places them at risk for law enforcement detection (Furnell, 2002). Thus, hackers tread a fine line between sharing information and keeping certain knowledge private (Jordan and Taylor, 1998: 764). Those who can successfully navigate this line can also gain some status in the hacker community. Demonstrating a commitment to secrecy is a benchmark for how well one lives up to a hacker ethic (Taylor, 1999). True hackers are capable of keeping secrets, creating an ideal for hackers to aspire to; thus secrecy reinforces and maintains boundaries between hackers (Taylor, 1999: 29).

Status is also tied to another important element of the culture: the idea of mastery (Meyer, 1989; Thomas, 2002). Mastery is a complex element that involves continual learning of new skills and "mastering one's social and physical environment" (Thomas, 2002: xvi; Rotundo, 1998: 347). Specifically, individuals demonstrate their ability to apply technical or social knowledge to the real world. For example, hackers taunt and challenge the ability of others while on-line (Thomas, 2002; Furnell, 2002). This frequently leads hackers to use their knowledge and skill to gain control over another individual's system, or take "root" (Thomas, 2002: xvi).

Such a demonstration of mastery can increase a hacker's status, as can displays of knowledge of hacker subculture (Meyer, 1989; Loper, 2000). When communicating with other hackers, especially through web forums, individuals may refer to the history of hacking, use slang, or reference other important parts of the hacking "scene" (Loper, 2000: 66). These references appear to illustrate the intensity of individual connections to hacker subculture and their relative status.

Though technology, secrecy, and mastery are the most frequently recognized elements of hacker subculture, many others have been suggested. What follows are elements identified in certain studies as part of hacker subculture that have not been reproduced by other research. For example, Jordan and Taylor (1998) suggest hackers share an "intimate and antagonistic bond to the computer security industry" (Jordan and Taylor, 1998: 770). This relationship is driven in large part by opposing stances on the ethical nature of each group's actions. Hackers perceive themselves as more ethical because of their efforts to keep information free, while computer security industry professionals believe their efforts to protect systems make their actions more ethical (Jordan and Taylor, 1998: 772). Thus, this discord unites hackers and establishes firm boundaries between these two related subcultures.

A similar conflict stemming from the generation gap between hackers has also been suggested as an important part of the subculture (Taylor, 1999: 32). Younger hackers view those in older generations as "has-beens," while older hackers are opposed to the current state of the computer underground (Taylor, 1999: 32). This causes misunderstandings between differently aged hackers and establishes boundaries between the age groups. In addition, younger hackers' activities produce opposition between the computer underground and law enforcement (Taylor, 1999). As new generations of hackers are fully versed in technology, social control agents at the lower end of the technological learning curve cannot keep up with their activities (Taylor, 1999). This is said to create a wide dislike of law enforcement by hackers, and may explain the antagonism between hacker subculture and law enforcement.

Beyond these components, other elements of hacker subculture have been identified (Loper, 2000; Jordan and Taylor, 1998). These concern discussions between hackers on various topics. For example, Loper (2000) suggests arguments over ethics and the definition of "hacker" represent important features of the subculture (Loper, 2000). Another study finds discussions on hacker motivations to be a critical part of hacker subculture (Jordan and Taylor, 1998: 768). Several motivations are mentioned, including an addiction or compulsion to hack, "curiosity as to what can be found" on-line, boredom with one's off-line life, a desire or attraction to the power felt when hacking, peer recognition, and a service provision to computer users (Jordan and Taylor, 1998: 768). Each of these discussions demonstrates ways hackers can measure themselves against others and gauge their status within the subculture. They also illustrate how hackers distinguish themselves from others.

There is one notable exception in the previous research, which suggests hackers do not constitute a subculture. Wysocki (2003) finds a large presence of individuals within the hacking community who want to improve computer security and create a "better, more stable, computer industry for all users" (p. 178).   This support of the dominant culture, he argues, keeps the community from being a subculture. However, Wysocki (2003) suggests malicious or deviant hackers and crackers could constitute a subculture (p. 179). The author is not sure, however, if crackers who do not comprehend their actions can be lumped together in a subcultural frame with those who intentionally hack and understand the illegal nature of their activities. Such confusion complicates his findings and leads Wysocki (2003) to provide no further elaboration on subcultural components.

Despite Wysocki's (2003) study, the image of hacker subculture is diverse but unified by the importance of technology, secrecy, and mastery. Though previous studies have given great insight into the values and beliefs hackers hold, they have some limitations that must be addressed. Specifically, all of these studies are constrained by time (Meyer, 1989; Taylor, 1999). Depictions of the subculture are only representative of certain periods, reducing their representative nature over time. While this is not a weakness per se, it is an important issue for all subcultural research.[4] Thus repeated examinations can improve our knowledge of hacker subculture and document new innovations and change.

In addition, previous studies of hacker subculture have been based largely on either interview data (Jordan and Taylor, 1998; Taylor, 1999) or analyses of posts to web forums (Meyer, 1989; Loper, 2000). The general use of single data sets in research may limit the representative nature of a study to very specific populations of hackers. Such research may not provide the same level of depth afforded by information derived from multiple sources (Lofland and Lofland, 1995: 71), and also is limited in its ability to comparatively examine the social organizational influences on subculture.

Three studies (Meyer, 1989; Loper, 2000; Wysocki, 2003) have used multiple sources in their examinations, but their analyses were constrained by either narrow research questions or sampling procedures. For example, Meyer (1989) focused more on examining the social organization of hackers than on researching the important components of hacker subculture. Also, this analysis used two similar data sources: 17 months of bulletin board posts between computer hackers, augmented by references to hacking and computer related publications. Loper (2000) developed comparative data

---

[4] This has been especially noted by gang researchers since the 1950's (see Short, 1958).

consisting of posts to a public e-mail listserv, hacker magazines and publications, and media sources. Also, Wysocki (2003) used a content analysis of news articles limited to five U.S. newspapers identified through a single search term, as well as four e-mail questionnaires completed by active hackers (Wysocki, 2003). However, when properly collected, multiple data sources can provide rich detail on the relatively hidden practices of hackers and hacking.

There remains a need to build upon these previous studies and examine hacker subculture using a combination of data sources. Because subcultural research considers how the values, beliefs, and goals of hackers structure relationships between individuals and the larger culture, this perspective allows us to understand how involvement in the subculture justifies engaging in hacking or related activities. Thus, this research will improve our understanding of both continuity and variation in the ideals valued by hackers and how subcultural membership affects their involvement in illegal activities.

THEORIES OF SOCIAL ORGANIZATION

Along with subcultural research, examinations of the social organization of crime inform our understanding of the social aspects of crime. Social organization frameworks provide a way to account for the level of deviant organization. This highlights the importance of organizations and associations in shaping both individuals and society (Best and Luckenbill, 1994). Most deviants have relationships with one another and form associations, especially in the context of subcultures. Thus, the social organization perspective allows researchers to consider how these relationships form, persist, and operate (Best and Luckenbill, 1994). This is extremely useful in understanding crime

and criminal organizations, and has been beneficial in advancing our understanding of hackers and their subculture.

Researchers have used social organization analyses to examine specific types of deviants (see Cressey, 1969; Zimmerman and Wieder, 1977), including the creation of typologies of deviance based on social organizational features (Clinard and Quinney, 1973). In addition, sociologists have developed organizational frameworks to examine deviant behavior, such as Cressey's (1972) analysis of criminal associations along a continuum of "rationality" (p. 16). The most rational associations have divisions of labor, rules that coordinate the behavior of each individual, and specific "announced objectives" the association seeks to achieve (Cressey, 1972: 11). This forms the basis for his six-point framework based on positions in a group's structure, ranging from commissioners in the most rational groups to guides in the least rational. Miller (1978: 295) also developed a framework to examine deviant work based on characteristics such as organizational rigidity and commitment to their activities.

Best and Luckenbill (1994) provide the most comprehensive theoretical framework for understanding the organizational features of deviant subcultures. Specifically, they provide a classification scheme for examining the organizational sophistication of groups, measured by "complexity, coordination, and purposiveness" (Best and Luckenbill, 1994: 11). Organizations differ from one another based on their division of labor, how frequently and successfully members of the group associate with one another, if they participate in deviance as a collective or individually, and how long their deviant activities "extend over time and space" (Best and Luckenbill, 1994: 12). These characteristics create a continuum of organizational sophistication along which

Best and Luckenbill (1994) classify five forms of deviant organization: loners,

colleagues, peers, teams, and formal organizations (see Table 1-1; Best and Luckenbill,

1994: 12).

Table 1-1: Best and Luckenbill's (1994) Social Organization Framework

Form of Organization	Characteristics			
	Mutual Association	Mutual Participation	Elaborate Division of Labor	Extended Organization
Loners	No	No	No	No
Colleagues	Yes	No	No	No
Peers	Yes	Yes	No	No
Teams	Yes	Yes	Yes	No
Formal Organizations	Yes	Yes	Yes	Yes

From Best and Luckenbill (1994) p. 12

Loners are the least sophisticated group, as they associate with one another

infrequently and do not participate in deviant acts together (Best and Luckenbill, 1994:

12). Colleagues are the next most sophisticated group, because individuals create a

deviant subculture based on their shared knowledge. This provides a way for individuals

to share information and evaluate others associated with the subculture (Best and

Luckenbill, 1994: 12). Despite this connection, colleagues are not very sophisticated by

measures of social organization: they do not offend together, have no division of labor,

nor exist over time.

Peers have all the characteristics of colleagues, and also offend together.

However, they are relatively short lived with no division of labor (Best and Luckenbill,

1994: 12). Teams are more sophisticated than peers. They last for longer periods of time

and have an elaborate division of labor for engaging in deviance (Best and Luckenbill, 1994: 23). According to Best and Luckenbill, teams tend to be relatively small in size, seek to garner money or power, and attempt to regularly operate while evading law enforcement (Best and Luckenbill, 1994: 44).

The formal organization is the most sophisticated deviant organization Best and Luckenbill include in their framework.   Formal organizations have all the elements of teams, as well as extended duration across time and space (Best and Luckenbill, 1994: 12). Best and Luckenbill (1994) also discuss an even more sophisticated and unique form of organization: the deviant community. They define communities as "groups which share a common territory and a higher degree of institutional completeness," meaning there are various institutions and resources that serve the interests of community members (Best and Luckenbill, 1994: 68). However, the deviant community is excluded from their framework as they are relatively rare and do not often develop because of the increased penetration of law enforcement in modern society (Best and Luckenbill, 1994: 72).

These categories provide a concise framework to examine how deviants connect and form into groups to engage in deviance.[5] This perspective recognizes the influence of subcultures and delinquent peer networks on deviant behavior and organization. Specifically, a subculture and social network of deviants are present in each form except loners. Thus, Best and Luckenbill's (1994) framework provides a way to differentiate between forms of deviant organization based on peer relationships and the functions and

---

[5] The use of Best and Luckenbill's framework in my qualitative analyses of the social organization of hackers is elaborated in Chapter Two.

structure of deviant groups. Such an approach is critical to any examination of the social characteristics of crime.

PREVIOUS RESEARCH ON HACKER SOCIAL ORGANIZATION

Best and Luckenbill's (1994) framework has been applied to many types of deviance, but only Meyer (1989) has directly applied it to hackers. Meyer (1989) developed a groundbreaking examination of hackers using this social organization framework, but little additional work has been done since that time. Meyer's (1989) study was ethnographic and involved 17 months of participant observation of Bulletin Board Systems (BBS), as well as e-mail, phone conversations, and communications with members of the computer underground. His evidence suggested computer hackers can best be classified as colleagues, because they developed a subculture centered on communications technology, creating a network in which they socialized and exchanged information with one another (Meyer, 1989: 63). This network also allowed hackers to indoctrinate new members into their subculture (Meyer, 1989: 63).

Still, Meyer (1989: 65) found that the majority of hacking was performed alone because of the sheer physical distance separating individuals on-line. Additionally, a great deal of competition existed between hackers because only a finite number of security flaws existed. This drove individuals to identify and exploit or fix these holes before anyone else (Meyer, 1989: 66). Thus, hackers were colleagues based on the Best and Luckenbill framework (1994), since they formed a subculture and shared information, but did not participate in hacking with others (Meyer, 1989: 63).

Meyer (1989) did suggest there were instances in which hackers resembled peer organizations, particularly when individuals organized into cooperative working groups.

These groups formed through private and public BBS (Meyer, 1989: 51). Through these BBS, individuals could connect and share information with others if they showed some knowledge of the computer underground (Meyer, 1989: 51). If one gained access to such BBS, they had the potential to join the group that ran it. This had a significant benefit: access to valuable information otherwise kept from the general hacker population (Meyer, 1989: 67). Since sensitive information could be abused or draw unwanted attention from law enforcement agencies, such knowledge was shared only between members of groups (Meyer, 1989: 67; Landreth, 1985).

Meyer (1989) found that associations with a group could lead to mutual participation in actual hacks against systems (p. 68). Such relationships moved these hacker groups beyond collegial associations to create peer organizations. Still, his evidence suggested most hacker groups were short lived, had small memberships, no set division of labor, were leaderless, and allowed individuals to do whatever they desired (Meyer, 1989: 73). These characteristics kept hacker groups from moving into greater levels of sophistication, and limited to peer associations only.

In fact, Meyer (1989) suggested that the organizational sophistication of hackers went no further than peer groups, and generally constituted "a transitory and limited 'criminal' enterprise" (Meyer, 1989: 80). This organizational assertion has been supported by some recent evidence, such as Slatalla and Quittner's (1995) journalistic account of the on-line feud between the hacker groups the Legion of Doom and the Masters of Deception. While the authors do not specifically reference Best and Luckenbill (1994), they consistently refer to these groups as gangs. They also detail how each "gang" recruited members, shared leisure time, and performed group hacks to

antagonize each other. However, since both the Legion of Doom and Masters of Deception were relatively short lived, they appear to fit the peer association category of Best and Luckenbill's (1994) framework. Likewise, Mann and Sutton's (1998) examination of interchanges between hackers in a UK web forum found "the structure and organization of the newsgroups in this study resemble earlier descriptions of street gangs"[6] (p. 220).

Despite tentative support for Meyer's (1989) findings, Best and Luckenbill (1994) caution that "a particular type of deviant can organize in various ways in different societies or at different times" (Best and Luckenbill, 1994: 13). Their framework provides ideal types for deviant organization. Thus it is possible the social organization of any given group is mutable over time and may even fall outside of their classification schema.

To this end, several researchers have built from Meyer (1989) to suggest that hackers have grown more sophisticated and may now in some instances constitute teams. In fact, several hacker groups appear to meet the team criteria, including the Chaos Computer Club, the Cult of the Dead Cow, and the l0pht (see Furnell 2002 for a discussion). However it is unclear how common this sort of organization is in hacker subculture. There is also growing evidence that hackers are involved in organized crime (Williams, 2001), and terrorist groups (Kleen, 2001). This suggests some hackers may now constitute "formal organizations" (Best and Luckenbill, 1994: 12).

---

[6] This structural similarity between hacker groups and gangs is relatively unsubstantiated in the text by Mann and Sutton (1998). Additionally, it is unclear why Slatalla and Quittner use the term "gang" throughout their research other than to create a sort of moral panic around hackers (see Thomas, 2002). Thus, the similarity between hacker groups and gangs is not fully understood or supported in the research literature.

One of the difficulties in determining levels of organizational sophistication is that formal organized crime groups appear to use hackers to perform certain actions. For example, entrenched and stable organized terrorist groups like Sri Lanka's Tamil Tigers have become involved in cyber-attacks against government resources (Computer Security Institute, 1998). However, the hackers responsible appear to be an offshoot of the Tamil Tigers, called the Internet Black Tigers (Denning, 2001: 269). Thus, it is unclear if they are part of a formal terrorist organization, or constitute a formal organization of hackers. There is also strong evidence hacker groups are coming together to create such formal organizations, as with pro-Islamic hacker groups in the Middle East (MENA Business Reports, 2002). This issue requires further examination, though, as it is unclear how common this level of organizational sophistication is within hacker subculture.

Given these questions, it is vital that the social organization of computer hackers be reexamined to build our understanding of the nature of hackers' organization level. Best and Luckenbill's organizational framework will be used to examine this issue as it is the most theoretically comprehensive model available. This will also allow for direct comparisons with previous research on hacker social organization. However, the inductive nature of this study provides a way to move beyond the parameters of Best and Luckenbill's (1994) ideal types. Thus my analyses can also generate new evidence of hackers' social organization.

CONCLUSION: AN INTEGRATED APPROACH

This dissertation examines both the subculture and social organization of computer hackers. It is critical that these two related issues be explored, as they represent important social aspects of crime. Examining hacker subculture can improve our

understanding of how and why individual behavior is shaped by subcultural norms and value systems. In turn, social organization research informs our knowledge of how individuals operate within the subculture both alone and in group contexts. Exploring these two issues allows this research to contribute to our knowledge of the social aspects of hacking. Furthermore, this can enrich our understanding of the social aspects of crime, especially offender networks, group participation in offending, and the influence of peers on behavior.

By examining these concepts in tandem, the current research sheds light on how the social organization of a deviant subculture affects its normative orders and vice versa. For example, the values of the subculture may place importance on the individual actor, rather than a group. In turn, this may lead deviants to infrequently form groups. Such lower levels of organizational sophistication may then impact the ability of deviants to share information or obtain needed resources.

There may also be some instances where the deviant act itself plays a role in shaping subculture and social organization. Researchers often examine the way behavior is structured by subcultural norms and values, or by deviant organization. However, the potential impact of behavior on the social aspects of crime is rarely considered. This is a critical issue in need of exploration, especially when accounting for technological innovations that alter the way deviant acts are performed. For instance, improvements in technology may simplify the way individuals engage in deviance may reduce the need to offend with others. These changes could also affect the way that deviants view those who use new tools and techniques within the subculture.

Thus, I will also attempt to assess the linkages between hacker subculture, social organization, and hacking, using conceptual questions from Best and Luckenbill (1994) to guide my analyses. These include how social organization, subculture, and hacking affect hacker ability, their "deviant careers, their rewards from deviance, and their responses to social control efforts," and how these issues impact social control agents (Best and Luckenbill, 1994: 9). This will expand our knowledge of the influences and connections between these sociological constructs and behavior. Such information will benefit criminologists and sociologists by elaborating the relationships between behavior, social norms and values, and the ways individuals connect to each other.

The subsequent chapters of this dissertation elaborate the findings of these analyses. Chapter Two provides an in-depth discussion of the methodology of this research. I discuss the data creation, sampling, and analysis techniques for all three data sets, including the limitations and benefits of each data set.

Chapter Three examines hacker subculture through the normative orders identified in the forums, interviews, and observations. Chapter Four presents findings on the social organization of hackers. This section considers the current state of hacker organization based on its complexity of divisions of labor, coordination of roles, and purposiveness (Best and Luckenbill, 1994). Chapter Five examines linkages between hacker subculture, social organization, and the act of hacking and their influence on one another. This chapter concludes with a summary of the research findings, and their contribution to our understanding of hackers specifically, and crime and deviance generally.

CHAPTER TWO: DATA AND METHODS

This dissertation uses analyses of three distinct qualitative data sets to examine three specific research questions. The first considers what elements characterize hacker subculture in social situations on-line and in the real world. Then, the current social organization practices of hackers will be investigated. Finally, this research examines the relationship between hacker subculture, social organization, and the act of hacking and how each influences the other. To address these questions, a set of strings from six hacker web forums, interviews with active hackers, and observations made at a hacker convention are analyzed using grounded theory techniques (Corbin and Strauss, 1990). The data are then triangulated to determine how each uniquely situated data set informs the interrelated research questions (Silverman, 2001: 307).

Such inductive qualitative analyses allow the identification of important issues and concepts to emerge from research subjects, providing rich insight into the experiences of hackers. Such methods are critical, as hackers comprise a hidden population which is notoriously difficult to examine (see Wysocki, 2003; Gilboa, 1996). I begin this chapter with a discussion of the ways concepts will be measured in this dissertation. Then, I address the rationale for using qualitative data to examine hackers. Each data set is detailed in turn, including its construction, benefits, and weaknesses. Next, I discuss the analysis procedures for each data set in full. Finally, I end the chapter by elaborating the triangulation procedures used in this research.

OPERATIONALIZATION OF CONCEPTS

I use very specific terms to measure subcultural elements and social organization. Subcultural values and norms will be measured using the concept of "normative order" (Herbert, 1998: 347). This is a "set of generalized rules and common practices oriented

around a common value" (Herbert, 1998: 347). An order "provide[s] guidelines and justifications" for behavior, demonstrating how subcultural membership impacts actions (Herbert, 1998: 347). This gives a dynamic view of culture, recognizing that individual behavior can stem from individual decisions as well as through adherence to subcultural values. Normative orders also provide for the identification of informal rules considered important by members of the subculture because of the values they uphold. Furthermore, this frame allows the researcher to recognize conflicts in the subculture based on the presence of contradicting orders (Herbert, 1998: 350).

Herbert (1998) provides little guidance on how to actually measure or identify normative orders, however his results were generated from ethnographic observations of police in a variety of settings. As such, I use grounded theory methodology to identify normative orders. Specifically, orders are inductively derived from the repeated appearance of specific actions, rules, or ideas in the data. The value of these concepts is generated from positive or negative comments of the respondents. In turn, theoretical links between these concepts are derived from the data to highlight the value or "normative order" that structures the behavior of hackers.

To assess hacker social organization, I use grounded theory methodology to derive concepts and information from the data, along with guiding questions from Best and Luckenbill (1994). Their framework was developed from inductive analyses of empirical research, considering how "deviant actors organize themselves to pursue their deviant activities" and how "these basic forms differ in organizational features, such as division of labor, coordination among the deviant actors, and objectives" (Best and Luckenbill, 1994: 9). They also asked questions to determine how these forms develop

and persist through the following questions: "what conditions shape the development and transformation of organizational forms," and "how do organizational forms change over time, and what conditions account for these changes?" (Best and Luckenbill, 1994: 9).

I apply these conceptual questions during my analyses, along with specific questions from a qualitative study of the social organization of gangs performed by Decker et al. (1998). Their research does not explicitly use concepts derived from Best and Luckenbill (1994), but they are concise and link well with this framework. Decker and his associates (1998) identified and examined elements of social organization that mirror the larger conceptual questions of Best and Luckenbill (1994). Thus, I synthesize questions from their research with Best and Luckenbill's (1994) concepts of complexity of division of labor, coordination of roles, and purposiveness to direct my analyses of organizational sophistication. These questions were used after the initial phases of data analysis were complete to refine my analyses, as they identify specific elements of groups, formal or informal regulations on behavior and relationships within groups, as well as relations across groups.

Specifically, the first series of questions I use centers around the *complexity of division of labor*, asking whether deviants offend together and the nature of their division of labor (Best and Luckenbill, 1994: 11). This includes questions about the presence of groups, their number of members, their relationship to one another, stratification, and the degree of role specialization. Second, the *coordination of roles* examines relationships between individuals (Best and Luckenbill, 1994: 12). Here, any codes or rules on the regulation of relationships, and how these rules are defined and enforced are assessed. Finally, *purposiveness* assesses relationships between groups and how they specify,

strive toward, and achieve goals (Best and Luckenbill, 1994: 12). These questions include any meetings between groups, their relationships, crimes committed by multiple groups, and any leisure time spent with other groups (Decker et al., 1998: 77).

Thus, I used questions derived from Best and Luckenbill (1994) in tandem with grounded theory methodology to examine the social organization of hackers. Inductive analyses of the data were performed to produce findings based on the respondent's repeated comments or observations relating to social organization. The value of a concept was based on the positive or negative stances of respondents to an issue. In turn, the results were compared against the Best and Luckenbill (1994) framework to assess the organizational sophistication of hacker subculture.

To assess linkages between hacker subculture, social organization, and behavior, I use questions from Best and Luckenbill (1994) for theoretical direction during my analyses. Their organizational framework provides some guidance on the impact of social organization on deviant behavior. Specifically, they ask "what are the consequences of organizational variation for deviants?"; "how does social organization affect social control agents' attempts to locate, apprehend, and sanction deviants?"; and "how does social organization affect individuals' deviant careers, their rewards from deviance, and their responses to social control efforts?" (Best and Luckenbill, 1994: 9). While these questions do not specifically address the influence of social organization on the subculture of a group, they highlight its effects on individual deviants. Since the values, norms, and beliefs of a subculture are generated in part by the way individuals relate to one another, it is also likely that the subculture of a group is influenced by its social organization.

At the same time, it is apparent that the subculture of a group has some affect on the determination of its social organization. To that end, I use a similar set of questions that provide a way to examine how the subculture influences individual behavior at the same level as social organization. Specifically, I consider the consequences of subculture on a deviant group's social organization, how the subculture affects social control agents' attempts to locate, apprehend, and sanction deviants, and how the subculture affects individuals' deviant careers, their rewards from deviance, and their responses to social control efforts.

Moreover, I use these same questions to examine the way that the act of hacking affects both social organization and subculture. I consider how hacks affect hacker social organization and subculture, as well as the way hacking affects social control agents' attempts to deal with hackers. The influence of hacking on individuals' deviant careers, their rewards from deviance, and their responses to social control efforts are examined as well. Using these questions allows me to examine the relationships between subculture, social organization, and behavior, including the ways they are connected to and influence one another.[7]

RESEARCHING HACKERS

To address the research questions of this dissertation, one must have access to hackers. This is rather difficult as they do not generally respond to solicitations for interviews (e.g. Wysocki, 2003). A few researchers have had success directly sampling hackers (e.g. Taylor, 1999; Woo, 2003), however unique sampling procedures have also

---

[7] I did not examine variation in the normative orders present across different levels of organizational sophistication due to consistent findings of collegial relationships across the data sets. This is elaborated in Chapters Four and Five.

been used (e.g. Loper, 2000). This includes on-line interviews (Wysocki, 2003), the use

of publications from the computer underground (Meyer, 1989), and posts from web

forums and list servs (Meyer, 1989; Loper, 2000). I developed three data sets to gain

hackers' perspectives on hacking using three data collection methods: a series of strings

from six hacker web forums, interviews with active hackers, and observations from the

Defcon 12 hacker convention.

Each of these samples is comprised of active or aspiring hackers. Criminologists

have sampled active offenders to better understand deviants and deviance but this can be

a difficult exercise, especially when dealing with hidden populations (e.g. Wright and

Decker, 1994; Adler, 1993). To gain access, researchers must engage in intensive

fieldwork, typically using qualitative research methods. There are significant benefits to

qualitative research as it provides an insider's perspective on the topic of inquiry. This

method also provides a fundamental means for understanding culture, particularly

subcultures (Silverman, 2001: 51). Most importantly, qualitative methods permit the

inductive identification of the values, norms, and beliefs that are important to the

individuals being studied. In this way, qualitative researchers can produce theoretically

grounded results as well as explore the contours of analytic frameworks and theoretical

hypotheses.

I developed multiple qualitative data sets to more fully address my research

questions. Each of these unique sources allows hackers to be viewed in different social

settings and from group and individual perspectives. Web forum posts highlight hackers

from a group context on-line, while the interview data provide a more individual

perspective considering on and off-line experiences. Observations made at the Defcon

convention stress the social experiences of hackers in a unique real-world setting, in both individual and group contexts. Triangulating, or comparing these data for similarities and differences, allows the distinct features of each data set to be connected while situating each in its specific social setting and context (Silverman, 2001: 235). This is a significant benefit, and has been used in previous research on hackers (see Meyer, 1989; Loper, 2000; Wysocki, 2003).

<center>**DATA AND ANALYSIS PROCEDURES**</center>

HACKER WEB FORUM DATA

The first data set I created is a series of posts to six different hacker web forums. Forums have been used with some success by researchers examining hackers, and have several benefits (Loper, 2000; Mann and Sutton, 1998). They can usually be accessed with little difficulty or interaction with the group. This reduces the potential for researcher contamination or bias that may arise in attempting to access hackers through participant observation or other naturalistic research methods (Lofland and Lofland, 1995: 74-75). Additionally, these forums provide almost instantaneous access to weeks or months of posts. They also include a variety of users with different skill levels and knowledge of hacker subculture.

Generally speaking, forums are on-line discussion groups where individuals can discuss a variety of problems or issues. An individual creates a post within a forum, asking a question or giving an opinion. Other people respond to the remarks with posts of their own which are connected together to create strings. Thus, strings are composed of posts that center on a specific topic under a forum's general heading. Since posters respond to the ideas of others, the exchanges present in the strings of a forum may

"resemble a kind of marathon focused discussion group" (Mann and Sutton, 1998: 210; Moore, 1995). Thus, forum discussions constitute a form of social interaction, providing information about the social world of forum users.

Forums were examined for normative orders indicating the values, beliefs, and activities that compose hacker subculture. These concepts were inductively discovered in the interchanges between hackers through grounded theory analysis methods. The repeated use of negative or positive descriptions for certain behaviors or ideas illustrated their value within the subculture. This same methodology was used to examine the social organization of hackers. Since forums demonstrate relationships between individuals, they provide information on the quality and strength of ties between hackers and specify what information hackers exchange in public forums.

Forum Data Collection

The forums identified for this data set were selected based on several criteria, including size, traffic, and public accessibility. Forums with both large and small user populations were identified to represent the range of forums currently operating on-line. Additionally, I selected high traffic forums with a large number of existing posts, as frequent posts suggest high activity. Finally, public forums were selected because they do not require individuals to register with the site to examine previous posts.[8] Thus, these forums would allow anyone -including myself- access.

I sought ten forums to serve as a data set for this analysis, however only six met the sampling criteria. This set was created using a snowball sampling procedure by

---

[8] Public bulletin board systems (Meyer, 1989), forums (Mann and Sutton, 1998), or e-mail lists (Loper, 2000) have been used in previous studies to examine hacker subculture. The data for this dissertation follows in this tradition.

searching Yahoo.com using the term "hacker web forum." Snowball samples are often

used in qualitative research (Wright and Decker, 1994; Decker and Van Winkle, 1996) as

a way to create a sample based on specific criteria when it is difficult to determine the

presence of given elements in a population (Maxfield and Babbie, 1998: 228). The

search term I used provided multiple links to forums, but most required membership to

examine forum posts. I searched the first publicly accessible forum generated by the

search and found it had a large user population with heavy traffic; I included it in this

data set.[9]

Based on the lack of public forums in the initial Yahoo.com search, I thought it

best to check the "Links" section of the site for connections to other public forums. This

first forum served as the start of the snowball procedure. Four links were found, and

their content examined. Two of these links went to private forums, while the other two

met the sampling criteria and were included in the data set. I then searched these two

sites' links and found five more forum links. Two of these links were inactive, while the

other three met my sampling criteria. The six forums that compose this data set include a

total of 365 strings, providing copious amounts of data to analyze (see Table 2-1 for

forum information breakdowns). These strings span two and a half years, from August

2001 to January 2004. Moreover, they represent a range of user populations, from only

20 to 400 users. Thus these web forums create a convenient, yet purposive sample.

However, there are several important limitations to this approach. Six web

forums have not provided a representative sample of all forums. For example, there are

---

[9] Unfortunately, the initial hacker group that was identified through a Yahoo.com search has recently renovated its site and altered the content. Since 4/1/04, the links and forum section have been removed, and there is no information provided regarding if and when this information will be restored. The web

currently 5,430,000 hits produced for the search "hacker web forums" on Yahoo.com.[10] This is a significant problem which is difficult to resolve. Clearly, examining all forums for their suitability in this research is beyond the capacity of a lone researcher. At the same time, the current sample provides so much data that including more forums would make it difficult to analyze with real rigor.

Table 2-1: Descriptive Data on Forums Used

Forum	Total Number of String	User Population	Timeframe Covered
1	48	109	11 months
2	50	20	2 months
3	50	101	9 months
4	117	179	2 months
5	50	110	6 months
6	50	400	30 months

It must also be noted that forum users are not representative of the entire hacker population. Instead, the data is biased toward hackers who are more likely to engage in on-line activities. This may produce an image of hacker subculture that is different from the experiences of hackers who do not use public forums. However, this forum analysis is triangulated with the other data sets. For example, I asked interviewees about their participation in public and private web forums. These questions provide information on the value of forums and the experiences others have taken from them. Such measures help balance the potentially skewed results of this data.

---

addresses and names of groups and users of all sites and forums used will not be provided in this analysis in an effort to maintain some confidentiality for the hacker groups and forum users.

[10] This number was determined on January 3, 2004 using the search engine www.yahoo.com. The actual number of forums included in this figure is unknown, but is indicative of the general volume of forums in cyberspace on a day to day basis.

An additional limitation is that publicly accessible forums allow individuals access to posts without being a member of the forum. At the same time, the forum administrators stipulate users cannot post illegal information or content. This limits the information exchanged and may reduce criminal hackers' use of these forums. Consequently, public forums are not representative of all on-line forums. On the other hand, novice hackers may be more likely to use a public forum. Individuals who are new to hacking are much more likely to begin by identifying public, rather than private forums (Landreth, 1985). This is a benefit for the project as these exchanges highlight the enculturation process of hacker subculture, which is key to this research.

The generally enforced and unwritten rule that all messages posted in these forums are in English is another important limitation to consider. This may deter persons who cannot read or write English from using these forums. Also, not all forum users have strong grammatical skills, creating some potential for misunderstandings and translation problems. This can complicate the use of forums by hackers and create problems within the data. For example, an unclear exchange may obfuscate what could be an important issue in the world of computer hacking. At the same time, forum users often ask for clarification if a post does not make sense. Thus, opportunities to explain and clarify comments by the posters increase the accuracy of the exchanges.

Relatedly, two strings in one of the forums were posted in German. A hacker group outside of the US ran this forum and some of its users found it easier to discuss certain issues in German. This introduces some potential for inaccuracy in my analysis as I do not speak or read German. Rather than introduce potential translation errors into

the data, I cut these two strings from the data. While this reduces the data's

representativeness, the cut ensures greater accuracy in my analyses.

A final limitation is that despite the public nature of these forums, if an individual

wants to make a post to a specific forum they are required to register with the system

administrator. This involves providing a user name, e-mail address, and in some cases,

creating a password for identity verification. Certain individuals may not be willing to

post if asked for such information, especially hackers involved in illegal activities. This

reduces the representative nature of these forums, and little can be done to resolve this

problem. Still, the information is relatively simple and could be easily falsified by

hackers of various skill levels. So it is possible these forums have a diverse user

population concealed through false identities. Despite these limitations, public forums

provide an easily accessible and extremely rich data set of social interactions between

hackers, highlighting the values and norms of hacker subculture and its social

organization.

Forum Data Analysis Plan

The first 50 strings in each forum were copied and saved to a word file for

analysis. The only exception is one forum with relatively brief strings. All of this

forum's available strings and posts were copied to ensure it was given equal weight in the

analysis. A total of 365 strings from all six forums were examined and coded. I drew

from grounded theory techniques (Corbin and Strauss, 1990), as its procedures permit the

researcher to "develop a well integrated set of concepts that provide a thorough

theoretical explanation of social phenomena under study" (p. 5).

This method requires data collection and analysis to proceed at the same time, allowing the researcher to gather samples based on categories and patterns present in data analyses (Corbin and Strauss, 1990). Furthermore, any concepts found within the data must be identified multiple times through comparisons to determine if they are in fact similar. In this way, concepts become relevant via repeated appearances or absences in the data, ensuring they are derived and grounded in the "reality of data" (Corbin and Strauss, 1990: 7). Grounded theory also requires that whenever concepts or comparisons appear, they be noted through unique memos and code notes (Corbin and Strauss, 1990: 10). They allow the researcher to keep track of all developments within the data and document how theoretical concepts evolve (Corbin and Strauss, 1990: 10). Also, the type of coding used changes as the theoretical development of the research becomes more complex. For example, the first phase of coding is broad but the subsequent phases are very focused to develop identified concepts into a cohesive theoretical framework.

Although grounded theory guided this analysis, I was not able to follow its methodology to the letter. The forum data was collected prior to analyses, and it was not feasible to revisit these forums for further strings and posts. Forum content can change daily with the addition of new posts and deletion of others. There is no guarantee that a string will be the same after a given period of time, making it difficult to revisit the data source. While this violates the grounded theory rule that data collection and analyses proceed at the same time, my analysis otherwise draws extensively from the spirit of grounded theory because I utilize its analysis plan.

Analyses began with open coding: all data were placed into specific events or incidents, then labeled and grouped into categories and sub-categories (Corbin and

Strauss, 1990: 12). The forum data were coded by hand rather than qualitative analysis software such as Ethnograph or Atlas.ti. The massive amounts of data would become unwieldy very quickly using analysis software. Instead, printed copies of each set of forum strings were read. Important passages were underlined or highlighted and assigned a specific identifying tag. The tags included Subversive Behavior/Ideas to identify any actions or comments that were rebellious, disruptive, or otherwise against institutions or the government. The Bad Behavior tag was used to encapsulate any illegal hacks, attacks, or otherwise deviant or criminal behavior by forum users. Comments highlighting the presence of variables or concepts of social organization were placed under the Social Organization tag. Information Sharing was used to identify instances of knowledge, files, or materials being transferred between individuals. The tag Strings Flamed was used for exchanges between individuals where coarse language or swearing was used to lambaste a user. Any question posted in the forums was placed under the Questions tag to consider the technical or non-technical nature of inquiries made. How To Use The Forum focused on comments to individuals explaining how to behave and interact with other forum users. The Hacker/Net Culture tag was used for all comments or ideas related to how individuals structured action, thoughts, or behavior especially as a result of the expectations of others. These tags were all inductively generated from the data rather than a preconceived framework.

Once this process was complete, the word file for each series of strings was opened and previously identified passages were cut and pasted to create new files for each tag. These new files contained only data appropriate to that heading. Then, axial coding began, testing the relationships between categories, subcategories, and the data

itself to further develop the identified concepts (Corbin and Strauss, 1990: 13). Each tag file was printed out, re-read, and re-coded to identify unique elements or subcategories in the tags. For example, the repeated appearance of specific terms like "script kiddie," "white hat," "black hat," and "newb" within the category Hacker/Net Culture suggest these are important labels within the subculture. The negative or positive context of these terms also helps to cement their value, particularly the negative connotations of "script kiddie." Also, certain passages were removed or placed under new headings during this phase because they were not relevant to their initial category.

Then the final selective coding phase began to determine how any categories or subcategories from previous stages could be linked to a "core category" of the phenomenon under study (Corbin and Strauss, 1990: 14). All axial coded tag files from each forum were combined into single file for each tag. This allowed the relevance of subcategories to be identified across the forums, and establish the key orders of the subculture. For example, the repeated appearance of debates over definitions for hacker across all forums highlights its importance in structuring one's behavior and actions. This procedure also structured my analysis of hacker social organization based on complexity of division of labor, coordination of roles, and purposiveness.

INTERVIEW DATA

The second data set collected was a series of in-depth interviews (N=13) with active hackers. Two methods were used: face to face and e-mail interviews. A fieldworker/key informant was employed and solicitations were made at a hacker group meeting to generate interviews locally. Hackers who could be met in person were asked to participate in an open-ended interview (see Appendix A for this interview guide),

lasting between two and three hours. These interviews (N=5) were taped and transcribed verbatim. Payments of $10 were offered after completion of the interview to compensate participants for their time.

To expand the sample size and likelihood of respondents, interviews were also conducted via e-mail (N=8). This method helped expand the pool of respondents beyond the Saint Louis area. Solicitations were posted to two e-mail list servs, and made verbally at the Defcon 12 hacker convention. These requests often precluded interpersonal contact or did not allow the respondent enough time to complete a face-to-face interview. Consequently, respondents were asked to engage in e-mail interviews using the same questions as the in-depth interview instrument (see Appendix B for e-mail questionnaire). This allowed respondents to complete the instrument at their leisure. Once the respondent completed the form, they returned it to me for analysis. A $10 payment was then mailed to the respondent as compensation for their time.

Regardless of the type of interview conducted, the instrument consisted of questions about individual experiences as a hacker, the presence of a subculture, and any associations or affiliations with hacker groups. This provided information on both the computer hacker subculture and its social organization. Questions were also posed to gain insight into how hacks are completed as well as what occurred during specific attacks. The development of skill, knowledge, and associations were also explored. Finally, subjects were asked about potential desistance issues and what law enforcement could do to effectively curb hacking activities.

Interview Data Collection

To initially collect data, a snowball sampling procedure was employed through the assistance of a key informant/fieldworker. Fieldworkers are common to ethnographic research as they often have ties to individuals involved in the behavior of interest (Maxfield and Babbie, 1998: 270). They can validate the identity of the researcher and their trustworthiness, drawing out participants. For this study, I asked a hacker I am closely tied to for assistance in this project as both a fieldworker and key informant. He was interviewed at the outset of the project and asked to help identify and solicit interviews. However, he was unable to generate any contacts willing to participate.

This quickly negated the potential for a snowball sample, so an alternative data collection method was used: spending time in areas frequented by offenders. This is time intensive, but an excellent way to gain access to hidden populations (Maxfield and Babbie, 1998: 271). After discussing the lack of subjects with the fieldworker, he suggested I try to gain access to a Saint Louis area hacker group. I tried to attend several meetings of the Saint Louis chapter of the 2600, an international hacking and technology group.[11] These meetings were held on the first Friday of every month in a public shopping center in a heavily trafficked area (Saint Louis Chapter 2600, 2003). Unfortunately, identifying the group in the crowded mall was difficult and I had little success. After several attempts over a period of months, I finally found a meeting consisting of two participants. In talking to the two young men, I was able to validate the

---

[11] The 2600 began in 1984 as a phreaking and hacking magazine. Groups and meetings exist to bring people together to discuss and learn about technology. These meetings are open to the public, including law enforcement and the media (2600 Meeting Guidelines).

group's sparse membership and lack of real meetings. I was able to elicit an interview from one of the attendees but this led to no further contacts.

Three other respondents were identified through word of mouth solicitations, however I was having little overall success. A few months into the data collection period, Dr. Vicki Sauter from the Department of Information Systems at UM-Saint Louis suggested she could assist in data collection. Because of her involvement in information technology, she was able to solicit interviews on two e-mail listservs for students and alumni from the University. Individuals who subscribe to these listservs have a strong interest in computers and technology, increasing the likelihood of contacting hackers. Her e-mail message detailed my identity and the project, as well as my trustworthiness.[12] Five individuals responded with an interest in completing an e-mail interview because of her solicitation.

To further develop this sample, I solicited attendees of Defcon 12. This international hacker convention allowed me to make contact with hackers across the country and reduce any bias caused by only interviewing hackers in one city. During the convention, I spoke with attendees about hacking and a variety of other issues. At the

---

[12] The following message was sent to two listservs by Dr. Sauter:
"I have a peculiar request (and you know that if I think it is peculiar than [sic] it is really strange!). If you are a hacker, or you have been a hacker, we need your help.
Thomas Holt is a Ph. D. candidate in the Department of Criminology and Criminal Justice at UMSL. He is examining hackers and hacking and would like to interview hackers regarding their experiences and opinions. These interviews can be conducted either in person or via e-mail.
Strict confidentiality will be maintained and your privacy ensured. All individuals who complete an interview will be paid $10 for their time, and $10 will also be paid for successful referrals.
IF you know anyone who is, or considers themselves to be a hacker and is willing to be interviewed, please contact him by phone on campus at 516-4914, or at 636-896-0923. Also, you may e-mail him at tjheeb@studentmail.umsl.edu mailto:tjheeb@studentmail.umsl.edu>.
Again, strict confidentiality will be maintained and your privacy ensured. To ensure that confidentiality, please contact Tom directly
. . . . there are some things I don't want to know.
Vicki Sauter

outset of any discussion, I identified myself as a researcher and explained the project.

After talking briefly, I would ask the person if they would be willing to participate in an

interview. Four individuals from around the country agreed to cooperate, all completing

the e-mail instrument.

The Sample

In all, I was able to complete 13 interviews. Demographic information was not

collected from e-mail respondents to increase their privacy. However, respondents did

provide some information in their completed interviews, such as gender. General

demographic data was directly collected during the face-to-face interviews. The data

suggests this is an all-male sample between the ages of 18 and 40. This is a largely white

population, and includes several individuals working in the Information Technology

field. The respondents come from around the country, including Missouri, California,

Illinois, Iowa, and New York.

I do not know if any women were included in this sample, but no one self

identified as female. The sample was not intentionally limited to males only, and this

may be due to relatively small number of women thought to be involved in hacking

(Taylor, 2002). Thus this result is not uncharacteristic of the general hacker community.

Additionally, no juveniles are included in this sample of interviews, though there are both

juveniles and women included in the forums and observational data.

There are two limitations within this data. First, the small sample size does not

provide a representative sample of hackers, though this is a routine problem in research

on active offenders (see Jacobs, 1999). In addition, the data comes from hackers who are

---

P.S. No, Tom is not a police or FBI "plant" . . . . he knows what he shouldn't ask you so that he doesn't
need to report you . . . and he doesn't ask those questions. He is a legitimate student."

willing to talk about their experiences with others and thus may not be reflective of more secretive hackers. Nonetheless, these interviews represent a purposive sample of hackers that were rigorously analyzed using grounded theory methods. These interviews prove information about individual impressions of the normative orders of hacker subculture. This is a different perspective from the group-oriented forum data and socially situated observational data. These hackers also provide in-depth personal experiences on the social organization of hackers. During the interview, respondents were asked about personal experiences with hacker groups, whether as a member or non-member. This generated first-hand information on the level of organization experienced by hackers.

Another important limitation is that there is no way to validate the criminal behavior of these individuals. None of the interviewees reported any arrests for their actions, precluding any sort of validity check through police records. The reliability of their responses is complicated without any sort of extant validation of behavior. At the same time, this is a common problem for research on active offenders. The respondents did not, however, report any outrageous or unbelievable behaviors. Furthermore I was not necessarily seeking criminal hackers. Many individuals engage in hacking activities without violating the law by attacking systems they own, or have been given permission to access. This is an important part of legitimate security development, often referred to as "penetration testing" (Penetration Testing Guide, 2004). As such, it was not necessary to identify hackers with real criminal histories and this does not negate the value of the interview data.

Interview Data Analysis Plan

The interviews were analyzed using grounded theory methodology in their entirety. Data collection was conducted concurrent with initial analyses, allowing the questions posed to be revised in later interviews to explore and refine specific concepts as they were identified in the data. The analyses progressed in much the same fashion as the forum data, using the same three-stage hand coding method. Open coding began by transcribing, printing, and reading each interview. Important comments from each interview were underlined or highlighted and given a specific identifying tag. Some of the tags used in the forum analyses were included: Subversive Behavior/Ideas, Bad Behavior, Social Organization, Information Sharing, and Hacker/Net Culture. A few of the tags could not be used as they were not appropriate for this data, such as Strings Flamed, Questions, and the How To Use The Forum.

The axial and selective coding stages further explored these concepts by first opening each interview file in word. Tagged passages were cut and pasted into unique tag files for further analysis. Subcategories and elements of each heading were identified to develop identified concepts. Selective coding entailed combining all the tagged files into a single file for each heading. This provided the opportunity for comparison to consider the significance of subcategories across all interviews. These efforts were used to identify the normative orders and social organization of hacker subculture.

OBSERVATION DATA

The third and final data source I developed were first-hand observations of hackers at Defcon 12, the largest hacker convention held in the US. This three day convention, held annually during the last weekend of July, draws participants from

around the world as well as researchers who use the convention as a way to gain access to the hacker population (e.g. Schell et al., 2002). There are multiple events, including panels of speakers and games where individuals and teams compete to hack different systems. A number of unscheduled events also develop after hours within the hotel confines. I made written and tape-recorded field notes, as well as photos for later coding and analysis. The key informant who assisted in interview data collection also attended the convention and made observations during panels and events. By attending panels separately and acting as a technical advisor, he was able to improve the overall coverage of the convention. Materials provided at the convention including papers, data, and the convention program were also included to examine the subculture and social organization of hackers.

These observations provide insight into hacker subculture based on hackers interacting in unique real-world social settings. The days and nights revolved around events that draw individuals together, creating ample opportunity to observe hackers exchanging ideas and engaging in social intercourse off-line. This data provides evidence of the normative orders structuring behavior and action within hacker subculture. In addition, groups of hackers attend Defcon to meet and in some cases compete against others in different games and competitions. Thus, while not representative of everyday hacker activity, Defcon provides multiple occasions to examine hacker social organization in action within social situations.

The Defcon Convention

Defcon is a hacker convention held each year in Las Vegas, Nevada since 1993 (Defcon, 2005a). It has always been open to the public, for anyone from law

enforcement to the technophile. Media agencies are also invited, including news stations, magazine reporters, and television networks. There is no pre-registration and attendees must pay $80 cash at the door. The fee provides attendees with a convention program, bumper sticker, and data disk containing data and files for panels, events, and other conference related materials. An official conference identification badge is also furnished, with a different design each year. No identifying information is required from attendees, however the conference identification badge must be worn at all times within the hotel to enter panels and events.

Numerous events were held during the conference from very complex technical presentations to a coffee-making contest. Panel presentations were held throughout the day on security issues, hardware hacking, phreaking, privacy, law, and more abstract technical applications. Presenters came from diverse backgrounds and include PhDs, security professionals, government agents, and hackers with specific interests. Anyone could present a paper, which had to be submitted to the convention organizers by a certain date. The panels were held in hotel conference rooms and a makeshift tent in the parking lot, and long lines were common to get a seat in very popular presentations. This made it difficult to attend all sessions; however they were broadcast on the hotel closed circuit television system and could be viewed from any hotel room or lounge.

Multiple contests took place both on and off the hotel grounds throughout the day. There were hacking competitions, as well as wardriving and Wi-Fi games. A robotics contest and lockpicking challenge were also held. Less technologically oriented events were organized such as trivia contests, a scavenger hunt, and shooting contest. There was also a small marketplace set up in the hotel allowing individuals to purchase equipment,

videos, DVDs, books, clothing, and various other goods. A dunk tank operated during the day to raise money for the Electronic Freedom Foundation. This was a not-for-profit donations funded group which defends and crusades for digital rights (EFF, 2005).

A rave called the Black and White Ball took place on Saturday night and DJs played music around one of the three pools in the hotel complex each night. Hotel guests also threw parties and gathered in different parts of the hotel day and night. Thus, this was as much a social function as an educational event providing a wealth of unique opportunities to observe hackers and hacking.

Observation Data Collection

To record observations at the convention, I took written notes, taped thoughts and observations on a digital voice recorder, and took many pictures for later reference. My fieldworker/key informant also attended the convention to assist in data collection. We attended panels and walked around the hotel grounds between sessions. I took notes during each panel presentation and consulted the key informant for clarification on technical issues. Written and taped observations were also made at the various games, competitions, and the marketplace. Everything from the music played, the behaviors of participants, attendance, and interest in the events were noted. Photos were also taken when possible of the competitions and the environment for later reference.

We also attended the activities each night and walked around the pools after the day's scheduled events ended. I stopped people whenever possible to chat and ask questions, especially at night when they were more relaxed. After identifying myself, I would ask for individual opinions on the convention and their experiences. Attendees were also asked about previous convention attendance, any thoughts on hacking, and

motives for attending the convention. Members of groups were questioned when possible to understand social relationships between individuals and groups. Solicitations for interviews were made when appropriate to a variety of attendees.

Data were also generated from the program given to all attendees. This document contains notes from the organizers and founders of the convention giving their perspectives on hackers and hacking culture. Credentials and information on all presenters and their talks are also provided. Pertinent information on the various competitions and events are printed in the programs as well. The data disk furnished by the conference organizers is also used in this analysis. Materials and data from all the panel discussions are provided in a variety of data formats. Unique files are also included, such as short films on hacker culture from the Defcon movie contest. These items provide a wealth of important data and are included in this analysis.

Observation Data Analysis Procedures

All data generated from Defcon were analyzed using grounded theory methodology. As with the forum data, only the analysis methods could be employed. I did adapt the sorts of questions asked while on site based on the information provided by respondents. However, full analyses were not performed while at the convention due to time constraints. Initially, all written field notes were typed and any recorded data transcribed and saved into word format, then printed for later hand coding. Program notes were also downloaded from the Defcon website and files from the conference data disk were opened and printed.[13] All these data were subjected to the three stage coding

---

[13] Many of the materials given to Defcon attendees are available on-line after the convention is over. Downloadable content includes a .pdf copy of the program and some of the presentation notes and materials, available at http://www.defcon.org/html/links/defcon-media-archives.html#dc-12.

process beginning with open coding. Comments and information within the data were highlighted or underlined and given an inductively generated tag. These tags were quite similar to those used in the interview data, including Subversive Behavior/Ideas, Bad Behavior, Social Organization, Information Sharing, and Hacker/Net Culture.[14] Each piece was read and initially coded during the open coding phase, then re-examined to identify subcategories during axial coding. Finally, the previously tagged files from each document were combined into single tag master files and coded to identify unifying themes or concepts during the final selective coding phase. This process provided great depth to my analyses of the normative orders and social organization of hacker subculture.

The data provides invaluable information from a unique social perspective. Also, seeing so many hackers in person provided insight into the relatively hidden hacker population. Men and women across age and race lines attended, making it somewhat more representative of the current demographics of hackers. This afforded the opportunity to speak with a broader spectrum of hackers than the interview data set. Finally, the conference allowed me to observe hacker groups in action, as well as in more casual social situations. Thus, this data provides tremendous benefits for this analysis.

These observational data have a few limitations that must be addressed. Since the observations were collected at a convention, it biases the data toward hackers who are willing to engage in social situations. The information gained may not be representative

---

[14] The similarity in tag labels across data sets was not an intentional decision on my part. Rather, it is the result of the encompassing nature of the categories created by each tag and conceptual repetition in the data.

of all hackers, particularly criminal or anti-social hackers. While this is a significant

issue, black-hat hackers who engage in criminal activities do attend this convention

(Shell et al., 2002: 226). Thus Defcon draws a diverse population from the hacker

community and provides a unique perspective on hackers.

Another limitation is the cost and distance of the convention that may preclude

some individuals from attending. This has particular significance for younger hackers

who may not have enough money to make the trip, or for individuals living outside the

United States. At the same time, there are ride and room sharing programs in place by

the convention organizers and attendees to help increase attendance (Defcon, 2005b).

Such measures reduce the travel costs incurred, making convention attendance possible

for more people. These limitations do little to diminish the significant benefits of this

data.

DATA TRIANGULATION

As a whole, these three data sets provide a detailed series of observations to

analyze the social organization and subculture of computer hackers, including individual

perspectives and group interactions. To utilize the full strength of these data, they were

triangulated (Silverman, 2001: 235). This is a somewhat contentious practice among

qualitative researchers, particularly when individuals combine different types of data to

validate one set over another (e.g. Garfinkel, 1967; Hammersley and Atkinson, 1983).

Data has a situated nature that can be lost through simple aggregation of data, which is

why there is some caution against this technique (Silverman, 2001: 235).

Triangulation must be performed carefully. Utilizing grounded theory

methodology to analyze each data set separately helps facilitate this process. I use the

results of each analysis to address the research questions, while keeping the data in its proper context. Specifically, I discuss the similarity of certain findings across the data sets, while identifying the unique nature of specific results. For example, hackers appear to share information across all three data sets, but each reveals a certain character of this process. The forum analysis suggests individuals must put forth effort to demonstrate their knowledge of hacking before information will be shared, while people freely shared files and materials in person at Defcon. Meanwhile, the interview data suggests hackers can take a variety of approaches to obtain important information, whether reading books or files on-line to asking teachers or friends in the "real" world. Thus, triangulation increases the depth of this analysis by considering similarities and differences that result from the contexts in which the various data was collected.

The remainder of this dissertation examines the findings produced by these analyses. Chapter Three considers the normative orders of hacker subculture both on and off-line. The unique nature of these orders in each data set will also be examined. Chapter Four investigates the social organization of hacker subculture using the Best and Luckenbill (1994) framework. Chapter Five considers the linkages between and influences of hacker social organization, subculture, and hacking on each other. Here, I combine the findings to develop a theoretical understanding of the social aspects of computer hacking. This chapter will also discuss the implications of the findings for future research, law enforcement, and crime generally.

CHAPTER THREE: NORMATIVE ORDERS OF THE HACKER SUBCULTURE

This chapter examines the normative orders of hacker subculture. Subcultural research allows for the identification of beliefs, goals, and values that approve of and justify hacking and related activities. As such, these facets of subculture are key elements in the transmission of subcultural knowledge between hackers, and thus may increase the likelihood of involvement in hacking. Previous research found that multiple elements compose hacker subculture, most especially technology (Jordan and Taylor, 1998; Taylor, 1999; Thomas, 2002), secrecy (Jordan and Taylor, 1998; Taylor, 1999; Thomas, 2002), and mastery (Meyer, 1989; Thomas, 2002). However, several other unique elements were identified that have not been replicated across studies (except Wysocki, 2003). The focus of this chapter is to examine and explicate the normative orders of the subculture and consider how they shape the social world of hackers.

I identified and examined these orders through inductive analyses of posts to hacker web forums, interviews with active hackers, and observations made at Defcon. Specifically, I found that hacker subculture is composed of five multifaceted normative orders, including technology, knowledge, commitment, categorization, and law. They generate justifications for behavior, affect attitudes toward hacking, and structure identity and status within the subculture. Also, the orders establish the boundaries of subculture and influence relationships between hackers, as well as with the larger culture. Finally, these orders give insight into changes in hacker subculture over time.

The contours and connections of these five normative orders are explored throughout the chapter. They share similarities with previous research on hacker subculture, though there were some contradictory findings within the data as well. Furthermore, certain orders, like categorization, were not present across all three data sets. Such issues are highlighted and discussed where relevant in the chapter. A thorough examination of the relationships between the normative orders ends the chapter.

TECHNOLOGY

One of the most significant normative orders identified is the relationship between hackers and technology. Hackers across the data sets clearly possessed a deep connection to computers and technology, which played an important role in structuring the interests and activities of hackers (see also Jordan and Taylor, 1998; Taylor, 1999; Thomas, 2002). Starting with the interviewees, three hackers such as Mack Diesel said their relationship with technology began by age five[15]:

> I was, yeah, I was about four and [my mother] would take me up to school
>
> with her sometimes and they had a computer there. If I got bored, she
>
> would let me, uh, fool around with the computer, you know, to keep me
>
> occupied, and after a while I enjoyed playing around with it.

Two others suggested they became fascinated with technology by age seven. Spuds wrote, "my Grandparents saw my aptitude for all things technical at an early age. At the age of seven, my grandparents decided to nurture that interest and aptitude by purchasing me my first PC." The remaining interviewees took an interest in technology during adolescence. Mutha Canucker wrote, "I got a computer when I was 12, and my interest grew from there. The more I played with it, the more I realized what I could do."

Gaining access to computers deepened hackers' interest in technology. Most were given a system either by a parent or loved one, but they were not always the best machines available. Dark Oz explained, "I really started with computers when I graduated from eighth grade and was given a Amstat PC20 8086 PC. It was slow, even by the standards of those days." Once they had a computer, hackers spent their time becoming acquainted with its functions in a variety of ways.

---

[15] Pseudonyms are used to refer to all interviewees unless otherwise stated. In addition, because of the relatively high number of males involved in hacking (see Jordan and Taylor, 1998; Taylor, 2002), masculine pronouns will be used unless it is known that the referent is female.

Video game technology commonly introduced hackers to the ins and outs of their system. Indiana Tones explained:

> It was a little tough, and uh, my mom basically worked with computers at work so she kind of helped me out with my games, getting games installed and told me like how to do things like that. And as I started playing more games I kept having to tweak the system settings to free up RAM and get the games to run because it was an old piece of junk computer, uh, because my parents couldn't really afford more. So then I started having to do research on how to tweak it out to get the best performance.

Adjusting their system in minor ways allowed budding hackers to improve their game play or compete against others. At the same time, it introduced them to a variety of skill sets. For example, some hackers learned to program their own games like Vile Syn:

> I was quickly introduced to the vast array of games that were made during that time, and how to execute them from the C64's [Commodore 64 computer] BASIC shell. By the time I was 7 the Computer Gazette was my newfound interest, full of raw BASIC code for games and applications. I coded around a total of 50 of these programs taking up to 5 hours to type each one.

The interviewed hackers' interest in technology quickly moved beyond games into the basics of computers through discovery and exploration. R. Shack wrote that, "continuing to play with computers got me further involved" in hacking, and interested him in the "capabilities that can be done with computers." Through understanding how individuals could be connected together through telephone lines or delving into how compression software functioned, budding hackers became interested in the many different facets of computer technology. This gave them an understanding and appreciation for a variety of technical skills such as programming, software, hardware, and computer

security. For example, Spuds "learned how to program the machine to make my own programs to do things for which there were no programs readily available to do. I learned how to fix the machine, upgrade the machine, and so much more."

Understanding the interrelated elements of computer systems is critical as a hacker's knowledge level directly relates to their ability and skill (see Thomas, 2002: 44). Therefore hackers must have an intense desire to understand computer technology. This was exemplified in the following comment from the forum poster Binkels: "Hacking allows people to learn more about computers. I am really into computers and try to learn as much as I can. I want to be a hacker to exploit systems/programs and using them to learn from and go further into my limited knowledge of computers." The urge to learn about computers and technology could be met through a variety of resources, especially web forums. MorGnweB wrote:

> You might want to remember that this forum is designed for people to ask
>
> questions, despite the fact that you can find almost anything on google. Soif [sic]
>
> we all should just searched [sic] for things ourselves thered [sic] be no forums.

Technical questions were frequently posted in the six forums analyzed. In fact, 387 questions were posted to start the strings, representing 72 percent of all strings analyzed. A range of questions were asked, including how to hack specific targets. For instance, Sp00n1uv wrote:

> I was told that netstat [program] would be the easiest way to grab ip's [Internet
>
> Protocol addresses] from yahoo messenger users but it seems to only grab a yahoo
>
> server ip and not the individual box [computer] ip. So i was wandering [sic] if there is
>
> another way to get ip's from messenger users or maybe a tool that could do this for
>
> me.I can get the ip if i get a cam[era] connected but dont know why just sending an
>
> im [instant message] wont allow this.??. I thought that im's were a direct p2p [peer to

peer] connection the same as a web cam.... Any help is greatly

appreciated.....thanx........

Posters, such as morpheuswannabe, also asked for assistance in identifying specific software or tools:

Ey [sic] people, I'm looking for a special keylogger. The keylogger must collect the

windows 98 login passwords and usernames. Is this possible. The keylogger must

a[l]ways start invisible when the computer is booted. Does anyone know such a good

keylogger and the place where I can download it?

Some individuals had questions about programming tools and exploits that included samples of their

coding procedures. Others wanted general information on hacking. For instance, g00fu5 wrote:

Im planning on printing out a bunch of different texts to print out and take around with

me so I can read them in my spare time. I was wondering if anyone could recommend

any good texts that are actually worth printing out for me. I am printing out the SQL

[programming language] white pages so far, but I need more. I am interested in just

about anything hacking-related, but nothing stupid (such as those netbios or subseven

tutorials).

Thus, the forums emphasized hackers' significant interest in and desire to comprehend technology.

Defcon also illustrated hackers' fascination with computers and technology. Most all of the

panels held during the course of the convention related to technology. Figure 3-1 shows the events

schedule of the first day of the convention where a wide range of topics were discussed, including

hardware hacking, phreaking, computer security, exploits, cryptography, privacy protections, and the

legal issues surrounding hacking and piracy. Furthermore, the data disk given to all attendees

contained programs and data relating to the panel presentations. This provided hands-on access to 13

different pieces of software and over 30 different applications from data on exploits to programming information.

Figure 3.1: Schedule for First Day of Defcon 12

DAY 1 FRIDAY JULY 30	TRACK ONE PARTHENON	TRACK TWO TENT	TRACK THREE APOLLO
11:00 - 11:50	Advanced Hardware Hacking Joe Grand	Freenet Ian Clarke	The First Inter'l Cyber War Peter Feaver & Kenneth Geers
12:00 - 12:50	Windows WaveSEC Deployment Paul Wouters	Message Security Jon Callas	Attacking Windows Mobile PDA's Seth Fogie
13:00 - 13:50		Real World Privacy nOnamehere	Buffer Overflow Peter Silberman and Richard Johnson
14:00 - 14:50	Introduction to Hardware Hacking Scott Fullam	Tor Roger Dingledine	We Can Take It From Here FX & Halvar Flake
15:00 - 15:50	Bluesnarfing Adam Laurie & Martin Herfurt	Tools for Censorship Resistance Rachel Greenstadt	
16:00 - 16:50	Hack the Vote Rebecca Mercuri & Bev Harris	CryptoMail Joshua Teitelbaum and Peter Leung	Wireless Weaponry The Shmoo Group
17:00 - 17:50		Mixmaster vs. Reliable Len Sassaman	Program Semantics-Aware Intrusion Det Tzi-cker Chiueh
18:00 - 18:50	RF-ID & Smart-Labes Lukas Grunwald	Snake Oil Anonymity Nick Mathewson	VICE—Catch the Hookers! Jamie Butler
19:00 - 19:50	Weaknesses in Sat TV Protection A	Identification Evasion Adam Bresson	Bubonic Buffer Overflow spoonm & HD Moore
20:00 - 20:50	Smart Card Security h1kari	NoSE BrEaK Thorsten Holz, Maximillian Domseif, Christian Klein	
21:00 - 22:50	Automotive Networks Nothingface	Leetest Link	TCP/IP Drinking Game

Technology structured many of the leisure events and competitions held during the convention as well. For example, the "Defcon movie channel" aired science fiction and technologically driven films such as *The Matrix* and *Equilibrium* on the hotel's closed circuit television network. A trivia challenge was held each night revolving around technology and hacker history. In addition, there were contests that required individuals to use technology in innovative ways. This was well displayed in the IP Appliance showcase where participants integrated fully functional computer hardware into common household appliances. Contestants also demonstrated their technological know-how in wardriving, WiFi, and robotics challenges.

The Root Fu hacking competition gave the most specific displays of hacking knowledge. This was an elaborately staged game where eight teams defended their own fictional savings banks. Teams were connected to a main router and scoring system, which would make deposits into each specific "bank". The system would try to retrieve its deposits every few minutes. Teams would earn a defensive point if the deposit was retrieved. At the same time, teams could attempt to steal other teams' deposits. If a team could register a stolen deposit with the scoring system and claim ownership until the retrieval time, that team could earn an offensive point. Penalties were issued based on the network traffic created by each team. The team who scored the most points through offense, defense, and penalty deductions won. So, teams had to win by defending themselves while hacking the other teams' systems.

The focus on technology even affected the décor of certain areas of the hotel. For example, the Root Fu competition was held in a room with a large pagoda in the center made out of motherboards and computer circuitry (see Figure 3-2 for detail). It served as the base of operations for the game organizers to disseminate information to participants and on-lookers. The pagoda also housed a large projection and sound system that ran videos, short films, and cartoons from various

websites on a floor-to-ceiling length screen. All these elements demonstrated the importance of technology in the activities and interests of hacking.

Figure 3-2: Root Fu Pagoda Made From Motherboards and Circuitry

The interviewed hackers also made some critical comments regarding the impact of changing technologies on both the act of hacking and hacker subculture. They suggested computers were generally not user friendly until the late 1980s and required some knowledge to be used properly. Mutha Canucker wrote about this issue, stating, "NOTHING WORKED RIGHT. And I mean nothing! No one tested software on anything other than an IBM or a Compaq, so if you didn't have such a system, and I didn't, software was the pits." Computer users during this period had to have some proficiency with their systems to perform basic tasks, let alone connect to other systems. Mack Diesel said:

> When I started out, the PC really was not ubiquitous. It was kind of uncommon to
> have a computer and a modem so the culture was quite different. People with a
> computer were a lot more knowledgeable about them and, uhm, you really had to

have some understanding about how things worked in order to connect to other

computers and make programs do what you wanted.

The advent of the Windows operating system and the World Wide Web in the early 1990s

changed the landscape of hacking. Bob Jones stressed this idea, saying, "hacking has changed so

much from back then to now with the advent of the Internet that it's not funny." These developments

made a wealth of information available on demand through search engines and web forums. Dark Oz

recognized the influence of these changes:

> How technology evolved has directly impacted how the hacker community has
>
> evolved. The very common BBSes and teleconferences that used to exist have died,
>
> now it's [sic] web pages and message forums, and hacking/computer security
>
> conventions.

These comments succinctly highlight the importance of technology for hackers and hacker

subculture. The normative order technology recognizes the significance of computers in structuring

the activities and interests of hackers. Furthermore, it supports the notion that hackers have an "easy,

if not all consuming relationship with technology" (Jordan and Taylor, 1998: 763).

KNOWLEDGE

Technology is also related to the multifaceted order knowledge. This order includes the

importance of learning, the acquisition of information, and how both of these issues impact the status

and labeling of hackers. Specifically, the hacker identity is built upon a devotion to learn and

understand technology. As one forum poster suggested, "if you want to be a hacker, then you should

start to learn. . . hacking is all about learning new stuff and exploring." Forum users and interviewed

hackers stressed the notion of curiosity and a desire to learn (see also Jordan and Taylor, 1998;

Furnell, 2002). For example, a forum poster wrote, "a hacker is someone who loves to find

alternative applications for any given technology, another word for this is inventor or innovator."
The interviewee MG also defined a hacker as "any person with a sincere desire for knowledge about
all things and is constantly trying to find it." Spuds also indicated in his interview that hackers have
a "natural curiosity about how things work and how they can be improved."

As a result, hackers spent a great deal of time learning and applying their knowledge.
Learning was one of the primary reasons to attend Defcon. Several attendees I spoke with said they
came to the convention to learn new ideas and refresh their skills. The importance of learning was
also detailed in the program by the convention organizer, The Dark Tangent. He wrote "I want a
party where all like minded geeks and innovators can chill out and swap ideas." Presenters provided
new information to attendees along with tools, security tactics, and creative applications of existing
products. Here, hackers placed great value on the creative use of technology and spreading these
innovations to others (see Jordan and Taylor, 1998: 763).

Most hackers stressed that the learning process began with the basic components of computer
technology. Forum poster dBones suggested, "you will have to start learning the basic techniques
and you will surely progress to be a better hacker." An understanding of the rudimentary functions
of computers provided hackers with an appreciation for the interrelated nature of computer systems.
Dark Oz explained his own learning experience:

> I tried to learn assembler [software that translates an assembly language into machine
> language]. Too low level for me, I was board [sic] with it, but in just trying to learn
> it, I taught myself a lot about how a PC works, how the processor and memory relate
> to each other, and this low-level of information has been extremely valuable to have.
> It's helped me to understand why things work the way they do, and why they were
> designed the way they were.

Similar comments were pervasive across the interview and forum data. Developing a broad

knowledge of systems, hardware, programming, and networking was extremely important to

interviewed hackers because it influenced their ability to hack. For example, 10 of the 13 hackers

indicated they had a variety of skills that allowed them to complete multiple tasks during a hack.

Such a diffuse understanding of computers and technology was beneficial, as Indiana Tones

explained:

> Everybody's got their own cup of tea, whether it be hardware, software, programming.
>
> You know, the IT people, they know where they stand. And most of 'em are always
>
> trying to absorb a little bit of the other stuff. Because the more you know about
>
> networking, the more that might help you program your program that's going to run
>
> over the network, you know. Uh, its just, the more you know about Windows, the more
>
> secure you can make your program.

Many interviewees reported developing their knowledge of computer technology on their own

through "trial and error" and "playing with computers." Experimentation allowed hackers to

determine the rules and parameters of software and hardware. Mack Diesel indicated, "I picked up

most of my knowledge and skill through reading a lot, taking classes, but primarily from just sitting

down and experimenting and seeing what works and what doesn't." j.Rose suggested he learned

through "trial and error, which I believe is the only effective way to learn computing techniques."

Hands-on experience provided a fundamental way to recognize the limits of systems and push beyond

them (see Jordan and Taylor, 1998: 764). As Mutha Canucker explained, "the motto was: try it, if it

works, write it down, if not, get out the DOS disks."

Forum users made similar comments on the importance of learning, especially on one's own.

The forum poster dBones wrote, "What I'm trying to get at is that you will become more

knowledgeable if you were to find out information by yourself and then teach yourself that information." This sentiment was also evident in the following exchange when a poster asked for information to learn to hack:

> **STfUser**: ok im quite new to this and need some mega help i need to know the
> basics of this hacking [I am] on my quest to becoming elite so if someone
> can help and give me the info and tell me where i can get it [information
> on how to hack] form [sic] i would much appreciate it.
>
> **3nf0r3c3r**: arrrrr how cute, seriously mate why would anyone want to go out of
> their way to help some random person hack computers?
>
> **H3H3**: Nah man, you want a teacher, you can pay lol [laughing out loud]. Besides
> that, read whatever you can get your hands on and understand the shit that you
> read.

Thus, forum users both explicitly and implicitly demonstrated the importance of learning on one's own. To that end, users provided web links in almost every string in each forum. These links provided specific information about an issue or topic discussed in the string without repetition or wasted time for the reader. Tutorials were also posted, giving detailed explanations on topics from programming to the use of hack tools. In some instances, users made actual programs available for download to help individuals learn.

Forum users also spent a significant amount of time discussing different hacking tools and methods. These conversations provided individuals with information on the quality of certain tools and tactics, including on-line wargames, software cracking tools, security software, port scanners, and password crackers. Each serves a specific purpose, such as port scanning programs that scan a system and provide the user with information on the Internet services that system uses. This

information can then be used to identify exploits on that system and attack it (Furnell, 2002: 119).

There were a myriad of tools available, and the devices a hacker could use depended upon their

choice of operating system, whether Linux, Windows, or Mac. Individuals primarily suggested a

tool or piece of software based on personal experiences and preferences. For example, Spanky

recommended the port scanner nmap, but was countered by Pi13driv3r who wrote, "frickin [sic]

linux users assuming everyone's like them… superscan 3." Thus, forum users were able to improve

their knowledge of the resources they could use through these discussions.

Hackers also made recommendations on training tools and techniques based on their personal

experiences. This was best exemplified in a discussion on which wargame users preferred[16]:

Frink: www.cyberarmy.com/zebulum

A friend found this site and joined, does anyone have nay [sic] info on

this, or the challenges used to advance.

C0m1cb00kgui: I think this one is better:

http://www.hackerslab.org/eorg/hackingzone/hackingzone.htm

I did a bit on Cyber Army and it seemed too cheesy for me. They got a little

carried away with the idealistic military rhetoric, in my opinion.

Here is the "hacking Challenges" links section of this site:

http://neworder.box.sk/codebox.links.php?key=36581

m013m@n: I'm sorry to say but hakcerslab [sic] kinda s**cks…

You should go for http://wargames.unix.se/index.php

In spite of such discussion, forum users recognized that individuals must decide what product

to use and learn how it functions on their own. Hackers must test different programs to see which

---

[16] Wargames are hacking simulators that allow hackers to practice and develop their skills on-line in realistic situations.

works best for their knowledge base and system requirements. Wingusdingus accurately described this process of trial and error during a discussion on security tools and firewalls:

> Bit Defender or maybe Bullguard, Winroute, Jammer, PC Internet control, Zonealarm, Visnetic [all are different pieces of software]. Everyone has their opinion on what wall you should use (mine being outpost pro) but the best way to determine what you need and like is to try them all. There are loads of walls that I have missed out so have a look around and see what you find.☺

These discussions illustrate that learning was not an entirely solitary enterprise for hackers. Rather, they used a combination of resources to learn new information and techniques. For instance, Kamron wrote that he learned about computers and technology when he "asked friends and did a lot of trial and error." It was evident across the data sets that social networks played an important role in educating hackers by introducing new concepts or providing tools and resources to hack. Vile Syn explained, "we [a small group of hackers] would constantly spend time trading pirated software, and discussing the next find. Here my interest in electronic engineering, cryptography and the lack of respect for software copyrights developed." Also, Indiana Tones explained that belonging to a 2600 club provided him access to a wealth of knowledge because the members were willing to share information:

> I would help someone learn to program in visual basic if they taught me how to do web page design, you know. Or this guy here will teach this guy web page design if that guy will teach him networking. And it was basically about sharing knowledge.

Hacker social networks[17] were not limited to physical connections. Bulletin Board Systems and forums allowed hackers to connect with one another and share information without actual face to face contact. Mutha Canucker discussed this issue in some detail:

> I made a lot of friends in much the same way as people make friends online now. Even though we all lived in the same city, we never saw each other. Where I live, public transit is bad and when your 14 you not just going to borrow the car for the evening. It was through these friends, one in particular, that I learned most of the techniques.

Status and Knowledge

The exchange of information between hackers did more than facilitate the learning process. When an individual shared useful information with others, they were able to gain status and respect. This was quite evident in the forums since individuals would post information in different forms. The quality of information or creative use of materials had a direct impact on how the provider was treated by others. For example, @bstin3ntc10wn posted a tutorial on how to use certain tools to determine if you have been hacked. Users gave the following comments in response to the tutorial:

> **Ajay:** Nice~
>
> **Aflackhata:** @bstin3ntc10wn: I never thought abuot [sic] using DameWare [a program] toview the registry remotely in that way. Interesting and good post… keep it up!
>
> **Ooooooooogg:** Tres Bien ☺
>
> Keep up the good work.

These posts recognized and complimented the creativity and skill of the tutorial provider because of the information provided. Individuals who shared sound knowledge were shown respect

---

[17] The importance of social networks in the development and education of hackers is explored more fully in Chapter Four.

for their ability (Thomas, 2002; Meyer, 1989). Conversely, information of questionable quality led to criticism and disrespect from other posters. This was exemplified in the posts following a tutorial on hacking a computer using a netstat program and an ftp connection. The information provided was not accurate, and users critiqued the poster:

sTeWiE: ROFL [Rolling On the Floor Laughing], nice effort at a tutorial but next time you may want to learn the material before writing about it

tracebustabusta: While it's appreciated that he tried to write one [a tutorial], never write about something unless you thoroughly understand it. That leads me to believe he wrote it to earn himself respect, rather than to educate someone else.

Thus, the quality of information hackers shared with others influenced their subcultural status.

However, most interviewees did not provide evidence that sharing good information with others had social benefits. While all had used forums or BBS at some point, they did not fully elaborate on their experiences. Instead, they discussed the utility of forums, their content, and the information they were able to obtain. The only notable exception was Dark Oz who gained status among his fellow hackers and received benefits for the good information he gave to others:

I could help a BBS Sysop [System Operator] fix a problem on his BBS, or install an addon [sic] for him if he did not know how, and I would then get co-sysop access. Once you're a co-sysop on one board, other people start asking you for help, and you often build a reputation as a helpful person. I would be helpful, and I would share programs, textfiles [sic], viruses, whatever it took, and people appreciated that, and I moved up the social ladder, continuing to learn as I went.

Hackers that applied their knowledge in specific and creative ways did gain status at Defcon. This was evident in the respectful way attendees treated individuals competing in the games at the

convention. For example, the Root Fu competition took place in a large room open to the public, however attendees were relatively quiet around the competitors and did not crowd their workspaces. Recognition and honor were also given to those who successfully applied their knowledge in the unique challenges during an award ceremony at the end of the convention. Contest winners were announced, brought on stage, and distinguished for their achievements. The crowd played heavily into this, shouting and clapping for the participants and victors.

In fact, the team that won the WiFi Shootout received multiple standing ovations from the audience. Contestants in the Shootout had to send and receive a signal between two antenna, which could be either homemade or store bought. The winning team gained the honor of the crowd by setting a new world record for the longest distance signal received between two homemade antennas. They also received a standing ovation because of their age: this team was composed of two 18 year olds and one 19 year old.

In addition, winners received prizes from competition sponsors, including books, products, and money. These prizes were a sign of respect, but did not have as much social cache as the awards given by the convention organizers. The winning competitors received a black conference admission badge and, in some cases, a black leather Defcon logo jacket. These items could not be purchased, and the black badge provided the recipient with free convention admission for life. Since the convention badge design changed each year, the black badge stood out as a symbol of achievement and ability. In turn, individuals who possessed these badges were shown respect by other attendees. For example, attendees surrounded an individual with a black badge at a party and asked a variety of questions to find out what he had done to obtain "the honor." The badge holder described his involvement in a competition the previous year, and the other attendees brought him drinks while he regaled them. Thus, black badges confer status and cache at Defcon.

A hacker's level of knowledge influenced the respect they were shown as well as the information provided in forums. When a question was posted, broad or vague information was given in response. This was because posters did not know the full extent of the user's knowledge base. The exchange became more specific when the individual provided some information about their knowledge of what they were trying to accomplish. For example, a poster asked about the use of a tool to perform a Denial of Service Attack and mentioned they were new to hacking. They received the following response:

Since you are a beginner, a DoS tool is not for you. If you try it and for some reason it works, the administrator of that server is going to track you down in a heart beat.

Unless he is an idiot. I suggest you start out with a basic port scanner and scan your friends computer for open ports. Get to know how those work first.

If an individual had a comprehensive understanding of technology, they could perform more complex hacks in a variety of ways (Thomas, 2002). Individuals who demonstrated they understood the technology they were working with received much more helpful information. For instance, MastRshke made the following post after a tutorial on cracking WinZip software using a debugging program:

Hey there Enforcer [the tutorial author].

I like really like this tutorial.

You should write more of them....

But I think I need to read a loot [sic] more of them before I begin with trying to crack winzip [sic]...

Funny cause I cracked the most of those programs from the link you gave me and some how I find something of it logic but this... Hm [sic] I don't find any logic in this

yet 😐

Is it not possible to crack winzip [sic] without W32dasm [a program to crack

Windows products]? Just by using Olly [a different program]...

Cause I like that program some how and would like to work a lot more with it.

I tried the best to follow your tutorial but... I didn't get it cracked 😐

Maybe I did something wrong...

I'll try again to morrow [sic]...

Enforcer replied, giving MastRshke the necessary commands to use the debug program Olly and

crack the software. This was due in large part to MastRshke's comments about his previous

attempts to crack software and use of the tutorial to understand the process.

Those with little technical knowledge had much less ability, limiting their method of attack

(Thomas, 2002). The following exchange regarding how to hack a security program reflected this

reality:

> **Hacboy:** Hey. Does anyone know how to disable deep freeze? Or once it's on, can it
>
> not be disabled?
>
> **Usor 9595:** Depends on what sort of things you can already do on the computer.
>
> Maybe the answer isn't disabling it, but deleting it.
>
> **Hacboy:** Hmm. I was thinking the same thing. I might try this, but I will have to
>
> think about it first and get a second oppinion [sic]. I don't want to skroo
>
> [sic] up dep [sic] freeze in a way I cant [sic] fix it.

The Defcon organizers and panelists also took the knowledge base of attendees into consideration

when planning presentations. The program notes suggested what background knowledge attendees

needed to understand the information and concepts presented.

For example, a panel titled, "Kryptos and the Cracking of the Cyrillic Projector Cipher", was "intended for a general audience with beginning to intermediate cryptographic experience." However, the panel "Introduction to Hardware Hacking", indicated it was "intended for beginners, but all experience levels will get a kick out of it." Considering the diverse nature of the panels as well as the number of attendees, such comments ensured individuals could learn at a reasonable pace and comprehend the panels. Furthermore, this detail allowed individuals to meet similarly skilled hackers and tailor the event to their own needs and interests.

A hacker's level of knowledge affected how they were viewed and labeled by others within the subculture as well. Several different terms were used to differentiate between hackers based on their skill level. Those with a deep understanding of technology were referred to as hackers. The extremely skilled hacker was also considered elite, spelled "1337", or 'leet (see also Thomas, 2002). However, a hacker with little skill who used tools and scripts was called a script kiddie (see also Furnell, 2002). New hackers or people with little knowledge were labeled noobs (see also Furnell, 2002). Both the script kiddie and the noob could be designated a "lamer" as a sign of disrespect based on their lack of skill. Since noob, script kiddie, and lamer had negative associations, individuals often applied these terms to the unskilled or uninitiated.

This process of applying negative labels was evident at Defcon. For example, in the program notes for the Root Fu competition, the game's organizers noted that there were qualifying rounds: "with only seven open slots, the registered teams had to pass qualification rounds, separating the script kiddies from the truly skilled." Also, several attendees I spoke with felt that the number of attendees with no real interest or understanding of technology or hacking was growing. As a woman who attended the convention for the past five years said, they "like to get dressed up, dye their hair, and freak out." These people were referred to as "scene whores" by more serious convention-goers.

In fact, several people I spoke with suggested scene whores made up a large percentage of the total Defcon population. One man went so far as to say, "only 25% of the attendees know what they're doing and the rest have no clue." Thus, the derogatory term "scene whore" allowed hackers to form boundaries between themselves and others based on their knowledge of hacking and technology.

A similar labeling process was evident in the forums, as individuals who had little knowledge of hacking were shown little respect and pejoratively labeled by others. This occurred in forums where individuals constantly attempted to obtain information from others. If a hacker asked an inappropriate question or demonstrated a limited understanding of technology, they were likely to be disrespected. Mack Diesel reflected on this process in some detail:

> When I did [post in a BBS or forum], I usually had enough information to phrase the question intelligently, to get some kind of feedback or answer. . . because if you didn't say things correctly then you could be in for it.

Thus, gaining information or assistance from others required great care. If a question was asked improperly, the poster risked losing status and respect. The following exchange gave an excellent example of this process:

> **FrankdaTANK:** I just started to do this shit to get back at someone that hacked me. How do I use sub7 [a remote administration tool]??all I know is u [sic] have to rename that .exe thing to say something that people would click. And then u [sic] have to send it to someone. Someone help me!!!
>
> **Htekkkk:** Be shot and therefore removed from the internet, lamer!

Such instances of labeling occurred in conjunction with flames, or "subtle varieties of insult and verbal jab" (Loper, 2000: 52). Flaming comments targeted individuals who were either new to the forum or hacking generally, as in the following exchange:

SUrEkIIL: Finally a English Hacking Forum. Im the newest guy. And probably the

kindest one you will meet. I will do anything to hack. IM a english teen in

america…I want to learn and learn more about hacking and hacking software. I

will only use it for good. only for good. Youcan count on me because i dun

[don't] believe in stuff like mis[c]heif or revenge.

Please, teach me how to hack. If you also have MSN Messenger, mine is...

I dun want to pay money for hacking material. Is it possible. At least teach me. I

will honor and cherish you. What else can I give?

Kenaan: learn a few things about the world and come back...

Bhutthassafas: why are there still people out there asking us to teach them how to

hack? i think this will never end.

Individuals might also be flamed if they asked about tools or techniques that were used by script

kiddies or lamers. An excellent example of such a flame came because of a poster named shackFU

who asked what he needed to do to get a sub7 server past anti-virus software. A poster replied,

"Thank God for the fact that your target is using anti-virus. Now be a good little script kiddie and

piss off. Asshole."

Individuals could also be indirectly labeled based on the way they were treated by others.

Repeated negative comments could lead to the perception they had no skill or were a script kiddie.

This was illustrated in an exchange where a poster asked about the use of DOS, a basic programming

language. In response, Batista wrote, "Jezus you wanne be a 1337 H4x0r [elite hacker] and you can't

even figure out a fkn [fuckin'] dos command?Just type shutdown in dos." Batista clearly mocked the

poster because of their lack of knowledge. Thus, a hacker's ability to understand and use computers

and technology plays a critical role in the status and respect they are given within subculture.

COMMITMENT

The elements that compose the normative order knowledge are also closely tied to the normative order commitment.   This order is multifaceted, referencing the investment one must make to become a hacker. Commitment to hacking structured individual behavior through continued study and practice of hacking techniques. Forum posters indicated it took a tremendous amount of time to learn to hack. Wiggum wrote, "For me… the most important thing to have if u wanna be a hacker is to 'love it' and [be] ready to give your time to learn and master it." Ashy Larrie also provided some insight:

> If you are just starting you might not have a clue what to learn, or what you should know. As for me, I just started reading texts for a long time. . .when I started I didn't understand most of what was said in the texts but just kept on reading, after awhile things become more clear and you get the idea of what hacking is all about. I think it's also better to find out yourself then if you would ask what is important to learn, because there are somany areas you do hacking in, and once you get the overall picture you can decide what interests you most at that moment.

While these comments echo elements of the order knowledge, the poster makes very distinct statements about the importance of commitment to learning. Specifically, hackers had to spend a significant amount of time learning and understanding computers and technology. Without such an investment of their time, hackers would not discover what issues they truly find interesting. In addition, continuous changes and improvements in technology compounded the length of time required to learn. Thus, hackers must be committed to the continuous identification and acquisition of new information. Mack Diesel emphasized the importance of commitment, saying, "the minute

you feel you've learned everything is the minute you're out. There's always something new to learn."

Moreover, this notion was present at Defcon, where participants sought to consistently provide cutting edge information. Attendees indicated they came to Defcon year after year to learn the latest information. Panel presenters demonstrated a commitment to sharing new information and tools in their talks and biographical notes. This excerpt from the Shmoo group emphasized this point:

> The Shmoo Group is a non-profit think-tank comprised of security professionals from around the world who donate their free time and energy to information security research and development. They get a kick out of sharing their ideas, code, and stickers at DefCon. Whether it's Root-Fu, lock-picking, war flying, or excessive drinking, TSG has become a friendly DefCon staple in recent years past.

Hence, the hacker subculture placed tremendous value on constant learning over time.

The order commitment also reflects the significant amount of effort applied to learn the tradecraft of hacking. It was apparent across the data that the time a person spent hacking improved their skills. Dark Oz reflected on this, writing, "You do this long enough, with many technical projects, and you begin to really learn a lot, and then it becomes quicker to pick up more things faster then you did before." Though this statement references the importance of learning, it clearly indicates the value of expending constant and consistent effort in the process of learning. In fact, a hacker's willingness and desire to learn affected the level of respect they received from others within the subculture.

If an individual did not prove they put effort forth to learn on their own, they were disrespected. This was most evident in the forums when hackers tried to obtain information from others. This exchanged highlighted the process:

Heshopolis: Hi, I'm interested in the OpenSSL Exploit [a script to attack a system].

　　　　But I don't have a nix [Linux] system to test it on The C [programming

　　　　language] code is on http://www.securiteam.com/exploits/5HP0P1F8AM.html

　　　　But I cant run it on a windows machine. Anyone know a binary?

　　　　Don't sta[r]t whit [with] that'juist [just] compile it crap of cource

　　　　[sic] that doesn't work, you'd spend a year looking for all the

　　　　includes.

　　　　Tnx

The Monkey: If you can't even fucking compile someone else's exploits, think about

　　　　actually learning what you're doing before you try doing it. It's clear you

　　　　know very little about C, which means you probably have no clue how the

　　　　exploit works, or even what it'll produce in the end. Get your head out of

　　　　your ass, fuck off, and read a book.

T0mp3t3r5: Get off your dead ass and code your own exploits, you fucking script

　　　　kiddie.

These comments plainly demonstrate the forum users' stance on the importance of understanding

how hacks actually work, which can only be gleaned through hard work and dedication. As such,

Heshopolis was flamed, disrespected, and derogatorily referred to as a script kiddie.

In addition, a hacker's commitment to learning affected the quality of information they were

given. In the previous exchange, no one shared information with Heshopolis because of his/her

comments. This also occurred when forum posters did not attempt to find an answer on their own

before posting, as in the following exchange:

Shark0: Hello. . . I was looking for some DoS [Denial of Service Attack] tools some

that can disconnect an IP.. I am wondering where I can find these at? Thanks

CaptainMurphymurph: If you can't even find a simple program, how do you expect

you're going to have the patience to attempt a hack? I suggest this small piece

of advice. Search again. Someone may be nice and past the link. But that's

only getting you one step closer when you're a hundred steps away.

CaptainMurphymurph berated Shark0 for demonstrating such a lack of effort and gave him no

information. This common occurrence revealed the relationship between a hacker's level of

commitment and the amount of respect they were shown.

Commitment also refers to the hours or days required to complete some hacks. For example,

Indiana Tones said "it probably took me a year" to hack his Internet Service Provider's mail server.

The process of a hack could be difficult and required creative thinking, as Bob Jones suggested:

You know to be able to do something like that [hack] you've got to take something

that's broke and fix it and taking something that's fixed and break it and that takes a

lot of perseverance. A lot of persistence. A lot of just, OK I've tried this, this, and

this. And where most people don't. Say yeah, I give up. I can't do it. You've got to

think OK, how haven't I tried? Or what can I twist a little to try a different way.

The challenging nature of hacking and the constant effort required became a motive for some

hackers. Completing challenging tasks fueled some hackers forward to persist in the face of failure.

Mack Diesel explained:

It's [hacking] is challenging and that is what spurs most people forward, is that

getting past a hard obstacle. You are going to see a lot of reading, and there are going

to be a lot of hard points and times where you fail. But if you succeed and try a lot of

different things by learning and doing, then there are going to be times when you get

up from the computer and clap your hands together and say yeah, you know. Getting

past something difficult is what will keep you going forward.

Defcon competitors demonstrated a high level of commitment to performing and completing

complicated lengthy hacks. Individuals spent months developing and testing equipment for use in

the games. This was especially true for participants in the WiFi Shootout who made their own

satellite receivers and equipment to send and receive a wireless signal. Participants spent many

hours in competition to win the contests. The Root Fu hacking challenge lasted for 36 straight hours

with no scheduled breaks for the competitors. Instead, teams had to manage themselves to ensure

their progress. Similarly, the Wardriving competition went on for 48 hours straight, from 1 p.m.

Friday until 1 p.m. Sunday. The winner spent the duration of the convention driving through Las

Vegas seeking out wireless Internet access points. In fact, only two individuals competed in this

game because of the intense commitment it required. Thus, these games demonstrated the skill of

each competitor and emphasized the value of commitment to hacking as an important way to gain

status within the subculture.

The value placed on the time and effort spent learning and understanding computers and

hacking may explain why nine of the thirteen hackers interviewed worked in the information

technology field, as did a substantial number of Defcon presenters. j.Rose commented on this,

writing, "most of the original hacking community… has gone on into big business and profitable IT

jobs…" These jobs are an excellent fit for hackers because of their commitment to learn and

understand technology and hacking. In fact, Mack Diesel related his experience as a network

administrator, saying, "I have spent nights at my work till 1, 2 a.m. trying to fix stuff, when some

jackass has been messing with your servers or trying to breach your security and at the end of the

day you go in late and you talk about it and you laugh."

Thus, commitment to hacking has a significant impact on the activities and interests of hackers. The importance of this order makes it clear why the forum poster WisdomCub3 wrote, "hacking is a lifestyle. Spend all your time on it and you will get better and better." Many forum users and interviewees echoed this sentiment, especially when defining the term hacker. For instance, MG wrote, "to be a hacker, you must live the life, not just play the part. You must be hacker in everything you do." In fact, Mack Diesel suggested a deep commitment to hacking is a "part of who they [hackers] are, it's their nature, so it be very difficult for that person to just turn it off like a switch."

CATEGORIZATION

Commitment, knowledge, and technology clearly affected the way individuals constructed their definition and meaning of the term hacker. This may explain why there was so much discussion over how to define hackers and their motives. Similar exchanges were also present regarding the use of specific hacking methods and tools by different individuals within subculture. These discussions constitute a critical component of subculture, forming the fourth normative order: categorization. The forum data informed much of this order as posters spent considerable time explicating who and what is a hacker. Aside from discussions of scene whores, such debate was noticeably absent from the Defcon observations. This could be due to the generally inclusive nature of Defcon and its focus on technical issues rather than cultural questions regarding who is a hacker. There was some evidence of this order in the interview data, particularly regarding the term "cracker" and "end user".[18]

Disputes over the nature of hackers and hacking allowed users to define and differentiate themselves from others within the subculture (see also Loper, 2000). The most spirited discussions

---

[18] There was some variation in the opinions expressed by interviewees, but their responses to the meaning of terms like black and white hat hacker were quite similar.

centered on how individuals defined a hacker. One began because of the following post:

> "When did you start thinking you were a 'hacker'?
> ☐ True lamer, spamming AOL/IRC
> ☐ Used a port scanner
> ☐ Found out how to connect to an open port with Telnet
> ☐ Used a lamer prog with 'hacker tools'
> ☐ Found out what an IP was
> ☐ Tried to download malicious scripts and only ended up hurting yourself
> ☐ Just assumed you were because you had a computer
> ☐ Other (describe in post)

This post accentuated behavioral measures or benchmarks in a hacker's development. Pages and pages of posts were made in response to this question, and similar discussions were present across the forums. Some posters felt that once they performed a certain task or understood a complicated process they could consider themselves a hacker. For example, in response to the previous post, ;unnammed; felt he would not be a hacker until he accomplished the following goals:

1. learn some programming languages

2. Read some material covering the subject

3. Learn some scripting

4. learn to fully understand Windows (any) and Linux

Many posters suggested there were attitudinal components of their definition of "hacker". This included a certain state of mind or spirit, such as Brainiackk who wrote, "the hacker seeks for knowledge, the unknown and tries to reach his own goals. That's the spirit." Curiosity and a desire to learn was an important part of most definitions of hacker, including para-nizoid who stressed, "In my opinion, a hacker is a person who is curious and enjoys exploring. Be that someones [sic] mind or someones [sic] computer hard drive." baXter echoed this sentiment suggesting, "I am a hacker, because I am willing to learn, fix my mistakes, and help others learn." The sentiment that hackers

help others learn was quite strong, suggesting this should fit within the order knowledge. However, it is also a distinct part of the order categorizations because many felt that this was an important component of their definition of hacker.[19]

In some cases, forum users held the notion of "hacker" as an ideal to strive toward, primarily because of knowledge. M0thm0nst3rm@n explained, "I think a real hacker never would call himself a hacker because no matter how much you know, you can't know everything and there's allways [sic] more to learn. I don't consider myself a hacker, I consider myself a n00b [sic] but I hope to be something close to a hacker some day." Similarly, the notion of being an elite or 1337 hacker was thought by many to be an impossible achievement. As jQuizon suggested:

id [sic] say nearly everyone who calls themselves 31337 is a liar I mean to call

your self that surely youd [sic] have to know nearly every thing about

programming hacking network system files hardware and much more.

Cerberus agreed with this sentiment, suggesting, "I really don't think I am '1337' or particularly a hacker. I just think of myself as being more experienced on computer. If you would as[k] me you won't every truly become 1337 as this, in my opinion, is impossible."

Individual variation in the definition of hacker led forum users to discuss whether they could call themselves hackers at all. A few posters felt others must identify them as a hacker to truly be a hacker. Gribblefan explained this perspective, suggesting, "I don't think you know when you're a hacker and you can't call yourself a hacker, its [sic] one of those titles that you can only receive from others." Recognition of skill was key to this perspective, as wAyNeBrAdY wrote:

I started calling myself a Hacker once some other people had called me one a few times. I

few computer specialists I worked with for a summer term at a government office a few

---

[19] The importance of hackers helping others to learn is also explored in Chapter Four, as it is an important element in hacker social organization.

years ago called me a Hacker, many of my teachers have called me a Hacker and I've had

friends call me a Hacker before. All of these people meant it in a positive way and

respected me for it, therefore I figured I really had become a Hacker.

However, most forum users did not agree with this perspective. Those who considered themselves

to be hackers made no mention of being labeled by others outside of the subculture. Rather, they

were hackers because of personal achievement or a motivation to learn and understand computers.

Hence, personal opinion significantly influenced the forum users' identity and construction of the

term hacker.

Individual conceptions also generated much of the discussion about what different types of

hackers do and how this relates to their label or title. This was especially true of the ideology or

behaviors associated with each type. Forum users spent a great deal of time talking about script

kiddies. This could be due to the sizeable presence of forum users who were new to hacking. These

users were strong candidates to become script kiddies because of their weak knowledge of

computers and hacking.

In fact, the name script kiddie was derived from their use of pre-made programs to execute

hacks. They relied on others to code and develop their equipment, which could be downloaded and

traded on-line. In fact, Mack Diesel suggested that because of the increased availability of

resources, "there are more script kiddies out there today, uhm, in fact probably more than ever could

have thought to be because of the changes in technology and the development of the Internet."

However, simply downloading and running scripts does not provide the script kiddie with a very rich

understanding of how to hack. The forum user cAuSeIsAySo explained, "script kiddies only use the

tools hackers code, mostly without knowing in detail how the shit works they use." Sir-loin

provided a concise definition: "script kiddies use the scripts of other people to harm any random

person. Script kiddies can be really destructive. Too bad."

Posters also felt the majority of malicious hacks could be attributed to script

kiddies. For example, 13v3ng3r wrote:

I think the people you call script kiddies have first started learning and once they

got that minimal knowledge to break into some computers they became obsessed

with that, in contrary to people who probably never stop learning.

In fact, forum users emphasized a connection between script kiddies and a remote administration

tool called Sub7. The program gives the user control over a system and is often sent to a target

disguised as an attachment or file they would be inclined to open (Furnell, 2002: 119). By clicking

on the attachment, the program installs itself and allows the sender to gain full access to the target

(Furnell, 2002: 119). Many forum users felt that script kiddies used the tool to maliciously damage

systems, despite the relative lack of consensus on tools as explored in the order knowledge. This

relationship was so strong that a poster made a photoshoped picture for one of the forums

highlighting the use of Sub7 by script kiddies (see Figure 3-3).

Figure 3-3: Illustration from Hacker Web Forum
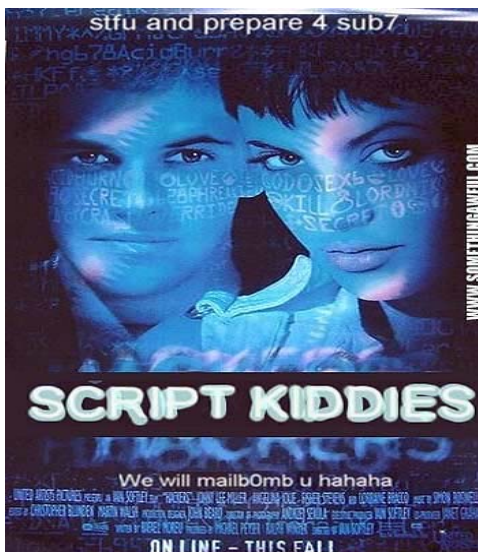
Interestingly, the base design for this picture was the poster from the movie *Hackers*. This was most likely a calculated decision by the creator based on the film's poor status in the hacker subculture. Indiana Tones succinctly explained, "well, the movie Hackers, anybody that thinks that that is a good hacking movie is completely wrong. I mean, that was just some idiot that could type like eight words a minute with really pretty neon light effects in the background, you know." Many hackers felt the stylized film misrepresented the image of hackers, drawing individuals into the destructive side of hacking (see Furnell, 2002; Thomas, 2002 for discussion). Thus, Sub7 users were often labeled script kiddies and their actions not considered true hacks. Phreaknwired elaborated this concept:

> The first time I ever thought I was a hacker was when I used 'hacker toolz' and port
>
> scanned someone…also when I had my hands on sub 7 and tried to use it (real script
>
> kiddie stuff). Then I realized how ****ing stupid that was and decided to go on and
>
> learn how to make my own progz [programs] for hacking into the system.

Preaknwired's comments highlight why many posters advised individuals against becoming script kiddies. Their actions do not provide them with an understanding or connection to technology. Slappywag explained, "don't become an Sk [script kiddie] it is illogical. It doesn't hold half of the internal enjoyment as knowing the stuff." Many users felt that kiddies were not hackers, though some suggested it was a step in the process of becoming a hacker. OvR18 wrote:

> I think most of the people who started getting interested in computers and/or hacking
>
> in an early state of age (like 12 or so) were script-kiddies/lamers how ever you wanna
>
> call it. Then or stayed lame theire [sic] hole life or developed to what they are now,
>
> newbies, neophytes (← spelled correct?) hackers. People have to start somewhere.

Several interviewees agreed with this notion, making reference to their own experiences. For

instance, Dark Oz stated, "I've been telling mostly stuff from the developmental period, which I

was more of a script kiddy then [sic] a hacker, but I was learning."

Because of their malicious behavior and lack of knowledge, the term script kiddie had a very

negative connotation among forum posters and hackers generally. This translated into a lack of

respect for these individuals, especially by older hackers because of their lack of skill and motives for

hacking. Vile Syn encapsulated this notion suggesting hacker web forums were populated by those

with "no idea about computers, but [who] want to gain information on hacking so they can show their

friends that they are cool for hacking someone's e-mail." These comments also support the presence

of generation gaps in the subculture between younger and older hackers (Taylor, 1999: 31-32).

While there was some consensus on the term script kiddie, there was less agreement between

forum users surrounding two of the main subtypes of hackers: white hats and black hats. Both were

very skilled types of hackers who engaged in different behaviors because of different ideologies. As

the forum user j@ck0 indicated, "the black hats use their knowledge to destroy things. The

whitehats use it to build things." However, there was some disagreement over the malicious nature

of black hat hackers. For example, kFowle3r responded to j@ck0's comments, suggesting:

> One thing about blackhats, its [sic] totally wrong that blackhats only use their
>
> knowledge to destroy..blackhats just hack ..not like whitehats which arent [sic] really
>
> hackers since they work against hackers, they build tools to stop people from
>
> breaking into systems etc ..blackhats break into systems but again its [sic] totally
>
> wrong that they hack to destroy, they hack for their own good, to learn and explore
>
> ..real blackhats don't "rm –fr/" [delete command] without a real good reason (besides
>
> script kiddie systems which is funny :>).. in fact the skilled blackhats don't destroy,

they keep root and even secure the box [computer] they got access to for free so you

got a hidden "security expert" which patches your box from the latest (even private)

bugs so noone [sic] else will get access.

These comments indicate white hats were active in the computer security industry, securing

systems from hacks. Black hats were more prevalent in the hacking community identifying

weaknesses and exploits for later attack. Beyond these concepts, arguments over the activities of

black and white hat hackers appeared to be based on personal opinion. This was apparent during the

following exchange:

> **Soezey:** i thought that#s no occupation [security and penetration testing] of a blackhat
>
> (maybe if he thinks he's an undercover agent...), maybe I'm wrong.
>
> **TomServo**: you seem to have a wrong view of blackhats dude ..blackhats do audit for
>
> sure ..i [sic] dont [sic] think that a whitehat audits much and codes exploits,cuz
>
> [sic] why code an exploit that you do not use ??? if whitehats code exploits then
>
> only for fame on bugtraq [a security website] and that's [sic] lame ..blackhats
>
> invent new exploitation tekneeqz [sic] etc we keep the scene going ..the
>
> whitehats just work on stuff to prevent us from exploiting certain things and we
>
> answer with something to circumvent their tekneeqz [sic].
>
> **Crow**: Even if you're a pure whitehat and doin [sic] pentests [penetration testing] for
>
> you're [sic] customers professionally, you've definetely [sic] at least present a
>
> scenario for exploitation and/or poc code [proof of concept code for exploits].
>
> Imho [In My Honest Opinion] it's just a false statement that whitehats don't
>
> invent new exploitation teqs [sic], it may be just the missing "slang" that
>
> makes you forget bout that.

New teqs [sic] come from new thoughts and even whitehats think (at least

sometimes)

A final subcategory of hacker present in the data was the cracker; however this type was

identified more often in the interview data. Forum users differentiated between hacks and cracks, but

spent little time elaborating the term cracker. On the other hand, the interviewed hackers were asked

how they defined this term, and there was a relatively even split in their responses. Six hackers

indicated a cracker was someone who tried, as Indiana Tones suggested, "to crack passwords, reverse

cryptologists, uh, the people that try writin' programs that do the serial numbers for the pirated

software." For these individuals, a cracker was involved in breaking protections to copy or otherwise

misuse software in much the same way as a software pirate (Furnell, 2002: 44).[20]

The other seven hackers suggested a cracker was a more malicious form of hacker, not

unlike a black hat or script kiddie. Spuds elaborated this concept, stating:

A cracker would be the SUREST word for someone who breaks into systems for

whatever reason. A hacker can be a cracker if his goal is to break into a system. A

hacker has a means and a goal and they have curiosity. Crackers are ONLY there to

break into a system.

His definition recognizes the similarities between the hacker and cracker, but also emphasizes the

cracker's desire to damage systems. In fact, the term "cracker" was developed by hackers as a

defense against media misuse of the term hacker (Furnell, 2002: 42). This may explain why Vile

Syn wrote:

Well, we all know the media's definition of a hacker, but the actual definition from the

computer industry's standpoint, a hacker is a computer enthusiast doing as much as

---

[20] A software pirate or "warez d00d" is a type of cracker who breaks copyright protections on software,
then distributes illegal copies (Furnell, 2002: 44-45).

possible to make things work for them. A cracker (media's hacker) is someone who solely dedicates their time to maliciously crack systems.

The variation present in the meaning of cracker illustrated the significance of individual opinion in the hacker subculture. Personal experience influenced how they defined themselves relative to other hackers. Labels may have specific connotations, as with black or white hat hackers, but individuals can accept or reject that meaning. In turn, hackers formed boundaries between themselves and others in the subculture based on their definition of hacker. The conflicted meanings suggest that there may be a lack of uniformity in hacker subculture, thus individuals create their own meanings for some terms. This may also explain the general disagreement over definitions for hacker within the larger research literature (see Furnell, 2002; Loper, 2000).

Interviewees and forum users also identified an important group existing outside of the hacker subculture called "end users." This is a term applied to the wider body of computer users who have a limited understanding and appreciation for technology, computers, and hacking. Interviewees suggested that the level of knowledge of most end users has decreased due to changing technologies. Computers and networked systems have become a common component of offices and homes around the globe. The ability of computer users has also increased with the advent of programs that simplify a variety of tasks; including banking, word processing, and on-line bill pay services. However most "end users" do not take the time to understand how their computer operates. Indiana Tones suggested they "aren't technically savvy and they're not really interested in technology. As long as their [Microsoft] Office starts up and they can do their word processing, as long as they can get on the server and do what they need to do, that's all they wanna know how to do."

Such a belief, coupled with the sheer number of computer systems, created more potential targets for hackers. This problem has been compounded by the use of Microsoft products.

Microsoft's Windows operating system software dominates the computer market, but has a great number of vulnerabilities and weaknesses. Most end-users own computers that run Windows software, increasing their attractiveness as targets for hackers. Mack Diesel explained, "most any Microsoft product is going to have a lot of vulnerabilities so they are really prime targets. Also, most people don't realize this and so they don't bother to fix their system or they don't even know that they are there."

The security deficit resulting from unconcerned end users with flawed software makes it much easier for hackers to gain access to a wide variety of systems. At the same time, Microsoft attempts to alert computer users to system flaws. Vulnerabilities discovered in Windows systems are usually publicly announced along with downloadable patches to fix the problem. Yet end users do not necessarily know how to update their systems or take the time to complete this task. As a result, hackers can obtain information on system vulnerabilities as well as potential target populations. Bob Jones detailed this process:

> You have, you know, millions and millions and millions of people that all have Windows that can tamper with it and find the next exploit. And, courtesy of Microsoft they publish all these exploits so as soon as they find one if you pay attention to their [the Microsoft] website then you could say, 'hmm, they say you've got a buffer overflow problem on this. I could find it.' Then you go through and you recreate that problem and you send it out and you hope that most people are as lazy as they are and haven't done the latest Microsoft update.

End users that do not fully recognize or deal with threats to computer security make themselves vulnerable to attack. In turn, engaging in malicious hacks has been simplified, altering

hacker subculture. Now script kiddies are much more likely to target Windows systems because they are readily available and easily attacked. Mack Diesel elaborated on this relationship:

> I mean script kiddies are the ones who are really most likely to target a Windows system for no other reason than they are full of vulnerability and these script kiddies have these tools and all they have to do is hit a button and the program searches for known fingerprints they are scanning and it says oh, well, this computer has . . . so why don't you use this virus and away they go.

Thus, the proliferation of technology and its effect on the larger population of end users has impacted the act of hacking and hacker subculture. Not only has it led to more potential targets, but also allowed hackers to establish boundaries between themselves and the larger culture. The order categorizations also includes boundaries formed within hacker subculture by considering how hacker identity is constructed. Individuals can establish their own definition for hacker through discussions on the meaning of "hacker" as well as motives for hacking.

LAW

The normative order law is reflected in discussions on the legality of hacking and information sharing. Justifications for the exchange of information which could lead to illegal behavior are also a part of this order. Moreover, law emphasizes the influence of law in structuring how hackers relate to individuals in and out of hacker subculture. Starting with the forum data, users often discussed whether some hacks or related activities were legal, and if they should be performed. There was a split between hackers who felt no illegal hacks were appropriate and those who viewed hacking in any form as acceptable. Such competing perspectives were addressed in the following exchange. An individual asked for information on a password cracking tool and how to use it. Pilferer answered the poster's question and gave an admonition that was quickly contradicted:

Pilferer: You do understand that using these password crackers on machines which you don't own or have no permission to access is ILLEGAL?

Leeter: Illegal ….

So is masturbation in a public place, but we don't get reminded of that every time anyone thinks about it do we? ;-)

In some cases posters inquired about the legal ramifications of certain actions, as in the following series:

b-RAK: . . .Finally is access through telnet [a program that connects a computer to a network server] legal if you got the ok form [sic] the person you were accessing or would your ISP [Internet Service Provide] know that you were using telnet to hack then boot you offline.

Z0r@K: Yes, ISP's can and will detect repeated scans, I suggest 7th sphere scanner if you're on a Windows OS [Operating System]

Yes they can and will detect it, and brute forcing is a good way to get caught.

Yes it would be legal if you got permission from the person but your ISP will still not like it.

Thunderclese: If you use nmap to scan a host, you can use the stealth feature that will keep you safe.

Portscanning isnt [sic] illegal anyway

When you get a list of open ports if you get any, you can use exploits to get root on the system

Linux is much better for this kind of things and much more of course. . .

Cl@r3nc3: That's untrue, depending where in the world you are then port

scanning IS illeagle [sic] so be carefull [sic]

It must be noted that in each of the previous examples, posters gave advice to perform a hack despite the potential legal ramifications that could result. In general, forum users provided information regardless of their attitude toward the law. This led to a contradiction in the process of information sharing. If an individual shared knowledge with possible illegal applications, they justified its necessity. Individuals across the data sets cited educating others as their main justification, as in this statement from a tutorial posted in one of the forums on macro-virus construction:

This is an educational document, I take no responsibility for what use the information

in this document is used for. I am unable to blamed for any troubles you get into with

the police, FBI, or any other department. Viruses are illegal to be spread, so this is

simply for theoretical purposes or testing in a controlled environment. It is not illegal

to write viruses, but it is illegal to spread them- something I do not condone and take

responsibility for.

Similar justifications were used at Defcon, especially when a presenter's content had rather obvious or serious illegal applications. An excellent example of this was a presentation titled "Weakness in Satellite Television Protection Schemes or 'How I learned to Love The Dish'". The presenter, Arturo, indicated, "I will not be teaching you how to steal service, but I will give you the background and information to understand how it could be done."[21] However, the second slide in his presentation provided the following information:

---

[21] The presenter's pseudonym has been changed from A to Arturo for readability purposes.

* Many topics covered may be illegal!

* "Except as otherwise specifically provided in this chapter any person who –

   intentionally intercepts, endeavors to intercept, or procures any other person to

   intercept or endeavor to intercept, any wire, oral, or electronic

   communication." 18 U.S.C. § 2511(1)(a). –

   http://www.4.law.cornell.edu/uscode/18/2511.html

* "No person shall intercept or receive or assist in intercepting or receiving any

   communications service over a cable system, unless specifically authorized to

   do so by a cable operator or as may otherwise be specifically authorized by

   law." 47 U.S.C. §553 (a)(1)-

   http://www.4.law.cornell.edu/uscode/47/553.html

* "Doing things that big corporations don't want you to do is illegal and

   immoral." A's take on the DMCA [Digital Millennium Copyright Act]

* Check out "DMCA, Then and Now" by Dario D. Diaz, Sunday at

   11:00 am for more info about the DMCA

This legal warning reduced Arturo's accountability for how individuals used the information

he provided. He simply shared his knowledge on satellite systems and television service. If

someone used the information to break the law, Arturo had clearly described the laws they could

violate by engaging in these actions. Just as with the warning in the macrovirus tutorial, he justified

sharing information that could be used to engage in illegal behavior, stealing satellite service, as part

of the pursuit of knowledge. This sort of justification was also evident in comments from Vile Syn:

"we also help the future 'hackers' who we feel deserve the knowledge by passsing down [hacking]

techniques." Mack Diesel used learning to justify his hacks as well:

I downloaded what's called a password dictionary file which contains hundreds of

words and used it to hack [a large public university in Missouri] password system

and I was able to get a number of passwords for accounts. I just let this program

run and I got the information for access to a number of different accounts. I never

did much with them, ahh, I just did it to see if it could be done. I wanted to know

how it worked, these, ah, these password files and I found out.

Interestingly, all of the hackers interviewed suggested that malicious, damaging hacks were

wrong and should not be performed. Some, like Mutha Canucker, took an ethical stance regarding

these hacks: "If you look at the Buddhist faith, which is possibly the most ethically correct religion,

one of the first 5 tenants is 'Do no harm to other persons.' If you maliciously break into a system,

you're going to do harm to another person." Spuds compared malicious hacks to "real world"

crimes, writing: "If you walked into someone's home and just break something. In the same respect,

it's not right to do the same thing to a computer. You can affect people's lives in this way."

In fact, taking a security job affected the interviewees' perspective on hackers and hacking.

Security professionals felt that hackers do not have the same skill or beliefs about hacking. For

example, j.Rose wrote, "those who are not working in legitimate security jobs tend to be, in my

experience, young left-wing radicals who have a fuzzy view of the world and wish to impose their

idealism on others." In addition, a job greatly reduces the amount of time an individual can spend

hacking and reduces their desire to engage in questionable hacks. Mack Diesel emphasized this:

"there's a saying it's hard to protest when you have to straighten your tie. That's part of the

responsibility you take as you become an adult . . . it doesn't allow you the kind of time you have as,

uh, as a kid." Indiana Tones made a much more specific point with regard to his career and hacking:

I know if it happens [being arrested for hacking] it's gonna go on my permanent

record and when I go to get a new job and I'm, you know, they do my security

background check . . . and they see, oh he got busted a couple of times. He's not

the one for the job. That's what keeps me from doing it [hacking] now.

At the same time, seven interviewees, including those in the IT field, felt some types of hacks

were acceptable. For example, Vile Syn said, "when dealing with hacking that isn't violating

privacy, it shouldn't be illegal at all." Hacks that did no damage or left no trace of entry were also

deemed acceptable. For example, Bob Jones said "even if you break in, you look around, and you

leave and they never know, who got hurt?" Dark Oz felt these sorts of hacks were a measure of

one's skill, writing, "It takes little skill to get into a system and cause damage, destroy, or make it

unavailable. The true skill is in getting in, looking around, doing whatever you want, but no one

ever knows you were there."

Furthermore, interviewees noted that hacking to identify flaws or improve security were

vital, justifiable hacks. Most hackers indicated hacking should not be illegal because of its benefits

for security. Kamron suggested, "breaking in to display exploits is not wrong." Indiana Tones

stressed, "hacking can be a good thing. Penetration testing, hacking your own network." Spuds

provided a very succinct explanation as well, writing, "to make hacking illegal would be asking the

makers of products to ignore their security problems. We find vulnerabilities in order to fix them.

Hackers do this because they want a product that is more robust. To make hacking illegal would be

asking them to ignore the pink elephant."

Nevertheless, forum users and the Defcon staff did not condone the exchange or supply of

overtly illegal information. In the forums, hackers eschewed posting blatantly illegal content and

forcefully explained this idea. This was in keeping with Mann and Sutton's (1998) finding that overt

"requests for illicit information are usually denied" (p. 216). For example, an individual proclaimed

himself, "the kind of hacker police really hate" and posted someone's credit card information. One

of the senior users posted the following comments in reply:

> No only do the police hate you Regardless if this is a honey-card and regardless if its
>
> good or bad to card (btw its bad), someone should delete it because it IS illegal and
>
> this is an open forum Go away

This standard also applied to information provided through web links. For instance, a poster gave

web links to tutorials and information on cracking e-mail accounts. The board moderator removed

the links from the post and commented:

> I would also like to add that we do not aid in the cracking of e-mails.
>
> The only assistance we offer for this is in the regaining of your own account. We
>
> advice [sic] if the account is really yours, to use the forgotten password option.
>
> Hotmail accounts are the ones most often wanted cracked. As I said, we only
>
> offer assistance in the regaining of your account. Hotmail has a special password
>
> reset feature which you can find here:
>
> http://registernet.passport.net/contactushm.srf?lc=1033&sd=p
>
> If your account was honestly hacked, and you seek actual help for getting your
>
> account back we're sorry.
>
> This same perspective on illegal behavior was observed at Defcon in a panel titled,

"Electronic Civil Disobedience and the Republican National Convention". The program notes

promised the panel would provide "tips on how to wage your own ECD [electronic civil

disobedience campaign] and how to participate in the upcoming actions to coincide with the protests

against the Republican National Convention." The speakers began by briefly describing the history

of electronic civil disobedience in a various countries. Then they called for attacks against a variety of targets during the RNC, including delegates and right wing businesses. Information was also given on generating media attention for instances of electronic civil disobedience through press kits and announcements.

The audience was initially receptive to their message, and even applauded at some points. However, crowd support shifted when the speaker stated they needed more foot soldiers "to take it to the streets" and "fuck up shit." He suggested there should be all kinds of disruption, including shutting off the power to Madison Square Garden, defacing web sites, and harassing delegates to "fuck them up."

One of the convention security staff's so-called "goons" [22] warned the panelists to stop saying "fuck shit up" because they were calling for involvement in criminal hacks and violent behavior. The talk was later interrupted by one of the convention organizers named Priest, who said the Defcon staff did not support or condone the actions of the speaker. He stated that engaging in any activities the panelists suggested was illegal and would lead to prosecution. Shortly after this interruption, the speakers were escorted from the stage by security and staff.

While this was a relatively unique event in the course of Defcon, it clearly demonstrated that certain types of information and behaviors could not be discussed openly. The same is true of the forums, as illegal information was not tolerated. Suggesting individuals engage in criminal activities or giving access to illegally obtained or questionable materials were not welcome in public settings on or off-line. However, sharing information that could potentially be used to perform criminal activity was acceptable.

---

[22] The private security staff at Defcon are called "goons." These are individuals who volunteer to work during the convention as security and assistants for presenters and staff.

The dichotomy of information sharing present in the hacker subculture may stem from the potential for law enforcement attention. Since anyone could view the content of public forums, it is entirely possible that law enforcement agents examined these forums on a regular basis. Limiting the amount of illegal information traded in the forums reduced the risk of law enforcement intervention. The same can be said for Defcon since it is open to the public. In addition, the convention organizers and staff did not permit individuals to engage in illegal behavior on the hotel grounds. Also, the convention organizers and some attendees noted that the presence of law enforcement agents was greater than in previous years. As a result, hackers limited the exchange of information in public settings and distanced themselves from anything overtly illegal.

Law enforcement interest in hackers and hacking influenced the way hackers related to others in and out of the subculture. This was particularly evident at Defcon because of their Spot the Fed Contest. Figure 3-4 provides the program notes for the game, which is referred to as "the ever popular paranoia builder," by asking, "Who IS that person next to you?" To play, anyone who felt an attendee was a federal agent had to alert one of the convention organizers that they had "spotted a fed." At that point, the potential "fed" was brought on stage before the crowd and asked a series of questions relating to security clearances, where they live, what type of car they drive, if they carry a gun, and more.

After responding to the questions, the individual was asked to reveal their identity. If the person was, in fact, a federal agent, both the fed and the spotter received t-shirts to commemorate the experience. There were at least eight "spot the fed" moments during the convention, and many referred to it as a Defcon tradition. It was also an important way to inform attendees about the presence of law enforcement. The game influenced the way individuals related to one another

during the convention. Attendees were much more careful about discussing illegal activities or

sharing information in the open.

Figure 3-4: Spot the Fed Announcement from Defcon 12

SPOT THE FED CONTEST

The ever popular paranoia builder. Who IS that person next to you?

Same Rules, Different year!

Basically the contest goes like this: If you see some shady MIB (Men In Black) earphone penny loafer sunglass wearing Clint Eastwood to live and die in LA type lurking about, point him out. Just get Priest's attention (or that of a Goon(tm) who can radio him) and claim out loud you think you have spotted a fed. The people around at the time will then (I bet) start to discuss the possibility of whether or not a real fed has been spotted. Once enough people have decided that a fed has been spotted, and the identified Fed (I.F.) has had a say, and informal vote takes place, and if enough people think it's a true fed, or fed wanna-be, or other nefarious style character, you win a "I spotted the fed!" shirt, and the I.F. gets an "I am the fed!" shirt. To qualify as a fed you should have some Law Enforcement powers (Badge / Gun) or be in the DoD in some role other than off duty soldier or Marine. What we are getting as is there are too many people with military ID angling for a shirt, so civilian contractors are not even considered!

To space things out over the course of the show we only try to spot about 8 feds a day or so. Because there are so many feds at DEF CON this year, the only feds that count are the kind that don't want to be identified.

NOTE TO THE FEDS: This is all in good fun, and if you survive unmolested and undetected, but would still secretly like an "I am the fed!" shirt to wear around the office or when booting in doors, please contact me when no one is looking and I will take your order(s). Just think of all the looks of awe you'll generate at work wearing this shirt while you file away all the paperwork you'll have to produce over this convention. I won't turn in any feds who contact me, they have to be spotted by others.

DOUBLE SECRET NOTE TO FEDS: As usual this year I am printing up extra "I am the Fed!" shirts, and will be trading them for coffee mugs, shirts or baseball hats from your favorite TLA. If you want to swap bring along some goodies and we can trade. I've been doing this for a few years now, and I can honestly say I must have ten NSA mugs, two NSA cafeteria trays, and a hat. I'd be down for something more unusual this time. One year an INS agent gave me a quick reference card (with flow chart) for when it is legal to perform a body cavity search. Now that is cool. Be stealth about it if you don't want people to spot you. Agents from foreign governments are welcome to trade too. If I can't be found then Major Malfunction is my appointed Proxy.

Furthermore, Spot The Fed created and reinforced boundaries between hackers and law

enforcement. While the game was "all in good fun" and performed in a tongue-in-cheek manner,

attendees took second glances at those who did not blend in with the crowd. Even I and my key

informant were asked about our status because we were taking notes and pictures of different events.

Openly questioning individuals about their lives clearly indicated who was a hacker and who was not.

The answers provided by federal agents gave hackers information about government agencies and

agents. Also, the public spectacle produced from a "spotting" ensured attendees would recognize the differences between hackers and law enforcement. Thus, this game provides some support for the notion that an antagonistic relationship exists between hackers and law enforcement (Taylor, 1999).

At the same time, evidence suggests that a bond is developing between these two groups, tempering this friction. This may be the result of increasing numbers of hackers with jobs in security and information technology (see Taylor, 2001; Schell et al., 2002). Government and industry have come to represent the lion's share of computer users and operate some of the largest and most sophisticated networks in the world.[23] They need trained security professionals to develop and protect their systems, and hackers make excellent candidates for these positions. This was most evident in a full panel was devoted to "Meet the Feds." Here, individuals from the Air Force, Department of Defense, US Postal Service, and other agencies fielded a variety of questions regarding law enforcement interest in hacking and potential employment opportunities with these agencies. Thus, there was some evidence of growing ties between law enforcement and hackers. In turn, this may explain connections that have developed between Defcon and the Black Hat Briefings security conference.

Black Hat is a security conference for IT professionals held three days prior to the start of Defcon. Though the name Black Hat is also used to refer to criminal hacking, this conference is meant for security professionals and those in the IT industry. Individuals could receive continuing education credits based on their attendance and credit toward certification as a Certified InformationSystem Security Professional (Black Hat FAQ, 2005). Interestingly, those who paid to attend this conference also received free admission to Defcon. As a result, an increased

---

[23] Attendees also noted an increased presence of businesses at Defcon. The number of businesses sponsoring prizes for the various competitions was given as evidence of this increase. Some of the sponsors included prominent technology related companies such as Symantec, Configuresoft, and Wired Magazine.

number of individuals attend both events. There is also evidence that the same panels are

held at both Black Hat and Defcon. When the schedules are compared, 26 of the 75

(35%) Defcon panels and presenters also spoke at Black Hat.[24]

Hence, some attendees suggested that the "underground" nature of Defcon has been

legitimized through associations with Black Hat, law enforcement, and the security industry. This is

an important issue, considering arguments made by other researchers regarding antagonistic

relationships between these groups (see Taylor, 1999). The relationships between hackers and law

enforcement may be changing.

CONCLUSION

Five interrelated normative orders shape the social world of hackers. Technology,

knowledge, commitment, categorization, law, and cultural shifts impact the attitudes, actions, and

relationships of hackers in myriad ways. These orders provide a way for hackers to define

themselves and the boundaries of their culture. They provide justifications for behavior, shape the

interests of hackers, and emphasize values that can be used to gain status and respect among their

peers. Moreover, these orders also gave evidence of contested issues within the subculture,

especially regarding definitions for hacker.

Similar to previous research, the relationship between hackers and technology is possibly the

most important order of hacker subculture, as it shapes and delineates other orders (see also Jordan

and Taylor, 1998; Taylor, 1999; Thomas, 2002). Technology is a primary interest of hackers,

leading them to focus on learning and understanding technology at a profound level. Thus, the

importance of technology is also intimately tied to the order knowledge. In fact, the desire to

understand computer technology justified hacking: to push all facets of technology to their limits to

---

[24] The Black Hat USA 2004 schedule is available at http://www.blackhat.com/html/bh-media-archives/bh-archives-2004.html.

know their greatest possible capacity (see also Taylor, 1999). Hackers also excused the exchange of information with potential illegal applications when it was given to educate others. In turn, engaging in illegal hacks could be legitimized when performed in the pursuit of knowledge.

Hackers based status and labels on their comprehension of and connection to technology. Individuals with demonstrable skill and ability received respect and were referred to as hackers. Those with little knowledge, but a desire to learn were often called newbies and shown little respect. Individuals who have little understanding of computers and no drive to increase their knowledge were considered script kiddies or lamers and shown tremendous disrespect and derision. The term "end user" applied to individuals with no strong comprehension of computer technology or interest in hacking. Hackers identified the boundaries of their subculture based on these labels (see also Loper, 2000).

Changes in technology have also had an impact on hacker subculture. User-friendly computers and the Internet increased computer use in government, businesses, and homes worldwide. Hackers have increasingly taken on the role of computer security experts to protect these systems and networks. Advances in technology over time have also simplified the act of hacking, requiring less knowledge to hack. In turn, older hackers created boundaries between themselves and the malicious script kiddies that have sprung from increased access to computers. This lends some support to the notion of a generation gap between hackers (Taylor, 1999: 31-32).

The normative order commitment is tied to technology and knowledge as well. Hackers placed significant value on continued learning and development of their skills. In fact, commitment may explain the increased number of hackers in computer security jobs. These positions allow hackers to gain a salary based on their skills and utilize their knowledge every day. Furthermore, this order engendered and justified sustained involvement in hacking and related activities to

develop their skill. Individuals who proved their strong commitment to learn and apply their knowledge obtained better information and more respect. This influenced how others viewed and defined their actions within subculture. This is quite similar to the concept of mastery described by Meyer (1989) and Thomas (2002), wherein hackers demonstrated their ability to apply knowledge to real world situations.

At the same time, individual opinion influenced the constructed meaning of the term hacker, as well as other labels within hacker subculture. There were many discussions between hackers regarding what constitutes a hacker, reflecting previous research which found a great deal of debate over the meaning of hacker (see Loper 2000) and different hacker motivations (see Jordan and Taylor, 1998). Some individuals considered themselves to be hackers because of their attitudes or beliefs about hacking, while others only considered the label appropriate after the completion of an act or acquisition of a skill like programming. Similar discussions focused on the subtypes of hackers, as with black and white hat hackers. This variation could stem from the value placed on learning to hack through self-teaching. Hackers were forced to become self-reliant and learn through trial and error and practice. As a result, a hacker's beliefs about whom and what constituted a hacker could be unique to the individual and dependent upon personal experiences. The only notable exception was the negative connotation of the term script kiddie. This may be an artifact of the status script kiddies have within hacker subculture. The disrespectful application of this label may lead hackers to avoid any potential recognition as a script kiddie. However, many hackers were likely to have been labeled a script kiddie at some point, since it represents an early phase in a hacker's development. This term created boundaries between hackers based on skill and behavior.

A similar contradiction is present with regard to hackers and the law. Hackers believe that malicious hacks are wrong, but the act of hacking should not be illegal because it advanced

computer security and improved technology. This provided a strong justification for involvement in illegal behavior. The illegal nature of hacking also created boundaries between hackers and law enforcement (see also Taylor, 1999), but this boundary is sometimes blurred due to increasing cooperation between these two groups.

Hacker subculture is structured by an interrelated set of normative orders that influence all facets of the social world of hacking. Technology, knowledge, commitment, categorization, and law affect the way hackers relate to one anther as well as the dominant culture. As with previous research on hacker subculture, these orders provide hackers with information that can be used to engage in and justify a variety of behaviors. However, I was able to find new relationships by examining subculture across three distinct data sets. Specifically, I found that normative orders had different influences in different social contexts, particularly the order categorization. Furthermore, my findings suggest that there have been innovations in hacker subculture due to changing technologies.

This study also demonstrates the importance of examining deviant or criminal subcultures because of the influence of subcultural norms and values on behavior. It is vital to examine the social relationships between deviants, as they facilitate the transmission of subcultural knowledge. In the next chapter, I explore the presence and significance of hacker social relationships as part of a larger examination of the social organization of hackers.

CHAPTER FOUR: THE SOCIAL ORGANIZATION OF HACKERS

The previous chapter considered the normative orders of hacker subculture, and how they structure the behaviors, attitudes, and beliefs of hackers. This gives some insight into the social aspects of hacking; yet it is also necessary to consider how hackers relate to one another within their subculture. Deviants often have relationships with one another and form associations which are used to transmit subcultural knowledge. Using the social organization perspective provides a way to consider how these relationships form, persist, and operate (Best and Luckenbill, 1994).

Examining the social organization of hackers demonstrates the various ways hackers form relationships with others and perform hacks (Best and Luckenbill, 1994). More than 15 years ago, Meyer (1989) found that hackers were organized as colleagues and, in some cases, peers. Their activities did not encourage greater levels of organizational sophistication. However few researchers have revisited the question of social organization in the intervening years, despite improvements in computer technology and its use. Here I explore hacker social organization using inductive analyses guided by conceptual questions generated from Best and Luckenbill (1994) and Decker et al. (1998) to assess the organizational sophistication of hacker subculture.

Best and Luckenbill (1994: 12) argue that organizations differ from one another based on their division of labor, how frequently and successfully members of the group associate with one another, if they participate in deviance as a collective or individually, and how long their deviant activities "extend over time and space." These concepts create Best and Luckenbill's (1994) continuum of organizational sophistication: mutual association, mutual participation, division of labor, and extended duration. The findings of this chapter are discussed in terms of this continuum, and combined with Decker and his associates' (1998) measures of complexity of division of labor, coordination of roles, and purposiveness.

I also compare the results against Best and Luckenbill's (1994) typology of loners, peers, colleagues, teams, and formal organizations. Recall that loners are the least sophisticated group because they rarely associate with other deviants, and do not participate in deviant acts together (Best and Luckenbill, 1994: 12). Colleagues are the next most sophisticated group, as individuals create a deviant subculture based on their shared knowledge. However, colleagues are not very sophisticated since they do not offend together, have no division of labor, nor exist over time. Peers have all the characteristics of colleagues, and offend together. However, they are relatively short lived with no division of labor (Best and Luckenbill, 1994: 12). Teams are more sophisticated than peers, since they have an elaborate division of labor for offending and last for longer periods (Best and Luckenbill, 1994: 23). Finally, formal organizations are the most sophisticated form as they have all the elements of teams, along with extended duration across time and space (Best and Luckenbill, 1994: 12).

This framework provides the basic structure for my examination of hacker social organization. In addition, I consider instances of groups that fell between or stretched the boundaries of the Best and Luckenbill (1994) framework. I end the chapter with a discussion of the limitations and complexities of this framework.

MUTUAL ASSOCIATION

To begin, Best and Luckenbill (1994) considered relationships between deviants to be the most basic component of organizational structure (p. 12). Deviants who do not communicate or associate with other deviants were considered to be loners, while relationships between deviants were indicative of potential collegial organizations. Turning to the current study, there were clear interpersonal relationships between hackers across all data sets. In all, 10 of the 13 (76%) interviewees said they had friends who hacked, though such friends represented a relatively small

percentage of their overall friendship network. Vile Syn emphasized this point stating, "I have a few friends that people would classify as 'hackers', but most of my friends really don't know much about computers at all."

Eight hackers described having "a few" or "two" friends that hack, like Bob Jones who suggested "there were like three or four of us who did this [hacking]." Often these friendships developed during school, such as R.Shack who hacked his school's computers with friends "to demonstrate to our admin. [administrator] of the vulnerabilities." j.Rose also mentioned this, writing "through school, I always had friends who worked with computers."

Only two interviewees suggested that most of their friends hacked. Spuds gave no actual numbers, but suggested "75% of my friends are hackers of one kind or another." Dark Oz also indicated that "lots" of his friends were hackers. This may stem from their deep involvement in the hacker subculture: Dark Oz was involved in a number of on-line groups and spoke at hacker conventions, while both Dark Oz and Spuds belonged to 2600 groups, which are offshoots of the 2600 magazine.[25] The mission of 2600 groups and meetings is to bring people together to discuss and learn about technology (2600 Meeting Guidelines). These two hackers' more intense involvement in the subculture may have influenced their social networks.

Social relationships were also evident at Defcon. For example, attendees spent a great deal of time together in the evenings drinking and having fun around the hotel's various pools. Parties took place inside individual rooms that often extended out into the adjoining hallways and patios. However, the unique interactions observed at Defcon were possibly an artifact of the situational

---

[25] The magazine is one of the foremost publications for hackers, providing technical and legal information in each issue (Furnell, 2002: 68). It is unclear how or why 2600 groups began, however it is apparent that the magazine's readership of hackers and phreakers began to meet with one another.

context of the event. Defcon has a very loose, festive atmosphere, complete with hotel

bars and vendors selling beer and hard liquor at various points throughout the day.

Yet the conference provides a way to facilitate mutual associations between hackers by

providing a place to interact with others in meatspace.[26] For instance, several attendees I spoke with

attended the convention just to catch up with old friends and make new acquaintances. The

convention organizers state on the second page of the program that they hope attendees develop real

world friendships. Defcon provides a significant opportunity to foster social relationships because

face-to-face interactions are relatively uncommon. So, despite the unique social climate, there were

demonstrable social relationships present at Defcon.

Relationship networks were also evident between forum users. Cordial social relationships

were present, as in the following exchange:

N30n3: HAS ANYONE SEEN ANY TRACE OF DAMAYER

LATELY…LOL (COMIC RELIEF)

MERRY CHRISTMAS ALL

N30n3

DAMAYER: Ha ha!

Merry christmas N30n3!

N30n3: ☺likewise. I thought it [unclear referent] was funny…any happy

new years asw ell[sic]!!

Forum users identified and related to one another based on their behavior and comments. If an

individual gave good information, they would receive thanks or praise from others. For example,

N30 made the following post after receiving useful information from Mr. Holmes: "lol thanks for the

---

[26] Meatspace is a term hackers use to describe the physical or corporeal world. "Meat" refers to the flesh and blood physiology of humans. This is in direct opposition to cyberspace, where individuals have no corporeal manifestation.

link Mr. Holmes. I researched this last night and had already written the batch file but that was still helpful." Individuals also gained a reputation if they were uncooperative or unwilling to help others. This was exemplified in a post lambasting a user named 0b10ng for his treatment of others:

> 0b10ng is one of those guys that come to this board dying to fit in somewhere or atleast [sic] have some sort of status somewhere because in life he is at the bottom of the totem pole..this is the same thing we learned in kindergarten, people make fun of others to feel better about themselves, or compensate for inadequate penis size;).

Users appeared to have relationships and contact outside of the forums through e-mail and instant messaging as well. Posters often put their e-mail addresses at the end of their posts, or in the text of a message. In some instances, posters discussed making outside contact in the forums, as in the following exchange:

> **Doocebigeleow**: My last question about this subject (hope that's allright.) You people gave me a lot of great programs to burn dvd's, but do you also know some programs with which I can burn burn-protected cd's (like games)(It's legal to backup your own games ☺).
>
> Thanx Doocebigeleow

> **B0b0f377**: I sent you a link [via] im [Instant Message] PM [tonight], let me know when you have read it.

However, the relationships between hackers were not necessarily deep, especially those developed in forums. Interviewees noted this fact, such as Mack Diesel who said, "there were some bulletin boards that I would visit and maybe throw a shout to some people if I recognized their screen names, but it's not like I had a bunch of people that I was really tight with." Bob Jones referenced the weakness of on-line relationships, stating: "Most of the hackers that I have ever talked

to on-line have been solitary people that, uhm, you see in passing then you don't ever hear from them again or, uhm, and usually it's because you've come to their attention for some reason."

The actual use of forums reflected the relatively shallow connections between users. In fact, the majority of all posters in the six forums posted less than three times. Table 4-1 details this trend, indicating that between 40 and 87 percent of all posters made less than three posts. This was common in web forums, indicating that the majority of forum traffic was composed of individuals making a relatively small number of posts (see also Herring, 2004). However, a small percentage of posters accounted for a high number of posts. For example, ten posters accounted for 48.6 percent of all posts in the forum with 101 users. In the forum with 21 total users, five posters made 73.8 percent of all posts. As such, the user populations from all six forums fit the "J-curve form" found in studies of differential participation in group activity (Robinson, 1984: 25).

Table 4-1: Forum Users Who Made Less Than Three Posts

Forum	Posters Who Made Less Than Three Posts	Total Forum Users	Percentage of All Posters
1	71	101	70.3%
2	131	179	73.2%
3	85	110	77.2%
4	8	20	40.0%
5	341	392	87.0%
6	78	109	71.5%

The depth of relationships between forum users was also affected by the use of multiple forums. It was clear that individuals used more than one forum based on comments from users like Hackwieser who wrote that he belonged to a forum on "a shitty site and everyone knows it, I'm SilentWolf from over there, hope you enjoy this place." Because two people in a forum could not

have the same username, it was possible individuals had multiple identities. In turn, this could

reduce the knowledge users had about each other. This was exemplified in the following post by

UltramegaChicken, describing their first hack:

> This isn't much, but just a while ago I was on a school computer, and I decided to
>
> rename the Recycle Bin. I soon found that Regedit [registry editing software in
>
> Windows NT] was disabled. Well, all I had to do was run Poledit [system policy
>
> editor enabling changes to be made in Windows setup] and disable all restrictions,
>
> which was just too easy. (Stupid admins…) Then I renamed the Recycle Bin,
>
> changed the BG< Screen Saver and practically everything else (including the
>
> password dialog text) to say "Hacked by HH" (which stands for HackHell, my other
>
> internet name). The teacher freaked the next day. I laughed myself silly, and they
>
> spent hours trying to fix it. BTW [By The Way], I notice there is (or was) a HackHell
>
> here (which is why I used UltramegaChicken), but just to clear it up, that wasn't me.
>
> I'm HH from [web link]. (Which is prolly [sic] where they got it cause they talk
>
> about hacking console video games there, and I happen to be an expert at that.)

The previous comments about expertise also emphasize the importance of going to more than

one forum. Membership in multiple forums was necessary because each had different

specializations and purposes. This was exemplified in a post from Toastly describing what

individuals should do to learn how to hack. He provided links to nine tutorials and forums, writing

"Besides reading all these newbie tutorials, you should defintely [sic] join some forums that will

help on your way. If you always keep to the n00b tutorials, then your knowledge will never increase

and you'll give up quite quickly." He then gave web links to each forum along with brief comments,

such as "The most formidable linux forum around. Although you probably won't start here soon, keep this one bookmarked as it'll [be] a huge resource later on."

Specialization within the forums was dependent largely on the members' knowledge base. If a user had specialized knowledge, they would often share it in posts. As a result, the overall nature of each forum was somewhat affected by the overall user population. For example, one forum had users with a good deal of programming knowledge; thus many technical coding questions were posed. Another forum had a range of user interests, and they provided five different tutorials to give detailed information on a broad range of topics. A different forum had five pieces of downloadable content, ranging from a cracked mIRC keygen to a user's MS Paint artwork. This forum also had cordial relationships between users, possibly as a result of its small user population. The remaining forums focused on general issues relating to hacker culture or basic hacking questions.

The use of multiple forums was just one way to obtain information on a number of different topics. Social networks between hackers were commonly used to share information, whether in person or on-line (see Meyer, 1989; Schell et al., 2002). For example, Defcon attendees sat at communal tables between and during panels discussing issues. Individuals lined the halls and common areas of the hotel with laptops connected together to share files and information. In much the same way, the main role of the forums was to provide access to information about hacking. A poster elaborated on this concept stating: "we are always trying to provide an atmosphere where any user can feel comfortable asking any question." As noted in the previous chapter, a myriad of questions were posed in the forums, and answers given in different forms, including tutorials, web links, posts, and downloadable content. Moreover, forums introduced users to the normative orders of hacker subculture, furthering hackers' development.

Nine of the 13 interviewees also reported using web forums or BBS to get information (see Meyer, 1989: 38). Through these resources, hackers could procure data on the weaknesses of targets. Spuds suggested he "would consult a resource online to find out about vulnerabilities of particular OS or service that was being run on that OS." Hackers downloaded different tools and software from on-line sources as well. Vile Syn explained that he would "dial into the BBS and interact with the BBS for files, documents, pictures, and anything else that was shared." Bob Jones also used on-line resources to get cracked software, or warez, explaining, "if you go on-line and you take the time to search for cracks and serial numbers… you can find a source with a lot of cracks, a lot of times they'll have tools to create worms or to install worms. Actual programs so you don't have to do any programming yourself." The availability of malicious software was noted by Dark Oz who recounted his experiences with BBS:

> With the modem I was exposed to more things, and had access to more software
> and text files. Since I had more things to play with and read, I continued to learn
> more and more. One day I found an underground BBS that had a virus collection,
> and so I downloaded a few and started experimenting with them on my PC, and
> collecting them (similar to how one collects stamps). I also collected Text Files,
> and other small things like that.

Hackers interviewed for this project also discussed the importance of sharing information. Almost all (84%) went to friends or associates for guidance and assistance when hacking (see also Schell et al, 2002). For example, hackers sometimes did not have enough knowledge to complete a hack on their own. Kamron described such an incident, when he "collaborated with friends who acquired information on the mechanics" of an on-line game server, enabling them to evade a ban in

place. Others simply exchanged information with friends to expand their knowledge of systems and technology. Indiana Tones explained this in some detail:

> I just liked listening to their [his phreak friends'] stories because they basically told me how the phone system works. See, I was more into computers and things…they always wanted me to make like good little boxes, [phreaking tool] you know. They were never really good at soldering or anything like that, so I mean I took that up and tried to help them out here and there.

Thus, it is clear that hackers do not operate as loners. They have developed a subculture with social networks that operate in both the real world and on-line. Connections between hackers, especially on-line, were not necessarily deep. Hackers used these social networks to share information including tools and techniques, as well as introduce the normative orders of hacker subculture. As such, hackers functioned as colleagues because of their mutual associations. This supports Meyer's (1989) claim that "it is impossible to be a part of the social network of the computer underground and be a loner" (p. 63).
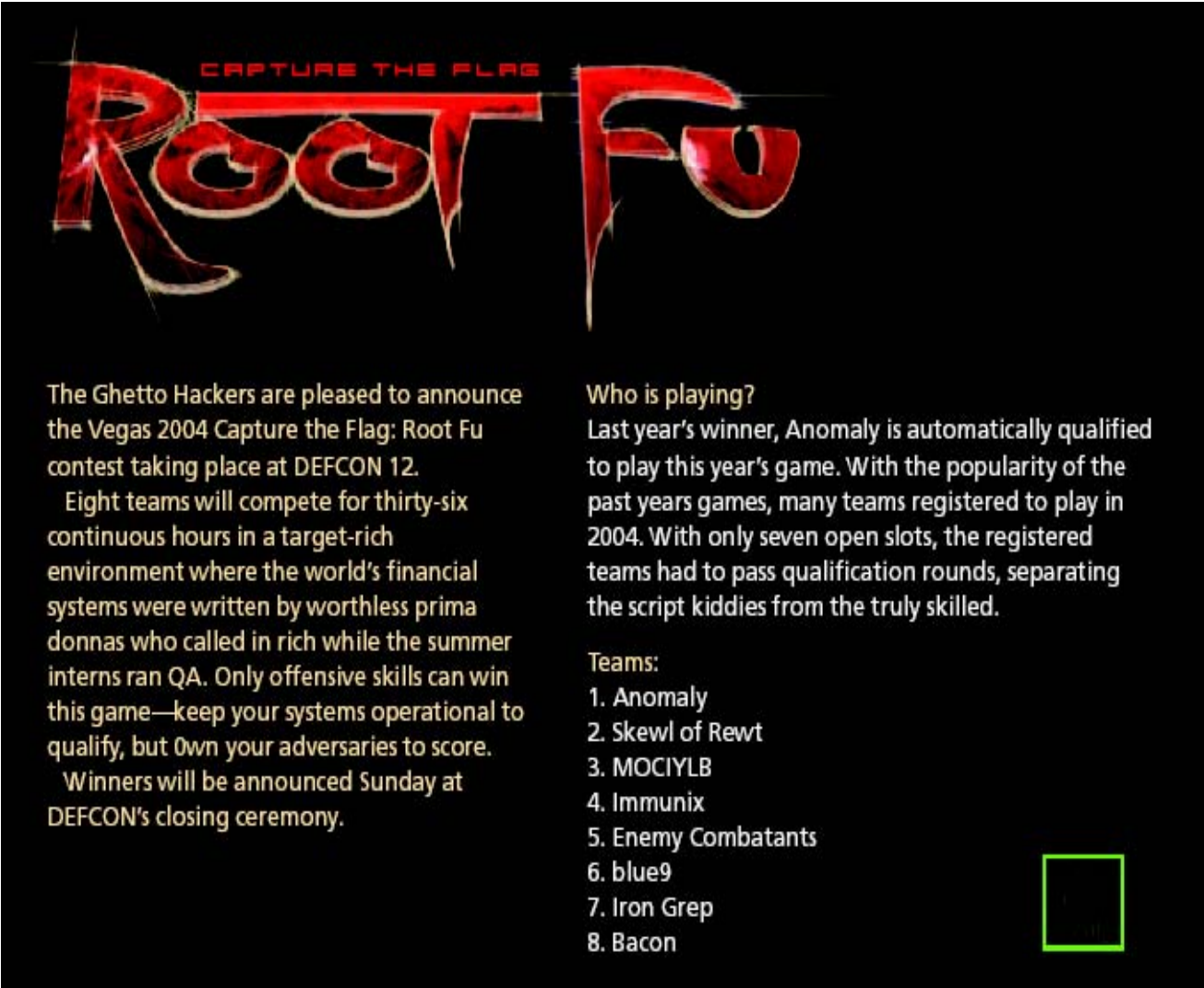
MUTUAL PARTICIPATION

While hackers had clear associations with others, there was some variation across the data regarding their mutual participation in offending. Hacker groups were prevalent at Defcon where 46 distinct groups were observed or mentioned in the program. For example, Figure 4-1 provides the Root Fu announcement printed in the Defcon program which describes the eight competing teams. The convention organizers also thanked the 50 or more Defcon groups operating around the world for their work and support. These groups are similar to the 2600 clubs, since the program indicates Defcon groups exist to "create a forum, with a place and time for people to meet exchange ideas, educate each other, work on projects, and have fun."

Groups of various sizes readily participated in the full gamut of events at Defcon. These groups formed prior to the convention, and were, in some cases, well established. Groups of three to four individuals commonly competed in different games, such as the three groups involved in the WiFi Shootout. One of the Scavenger Hunt groups named Pot Broccoli also had three members. Larger groups were present in Root Fu, like the Skewl of Rewt which had 13 members. The Salt Lake City and San Francisco 2600 chapters that helped implement certain games at the convention had 13 or more members as well.

Figure 4-1: Root Fu Program Announcement

The Ghetto Hackers are pleased to announce the Vegas 2004 Capture the Flag: Root Fu contest taking place at DEFCON 12.

Eight teams will compete for thirty-six continuous hours in a target-rich environment where the world's financial systems were written by worthless prima donnas who called in rich while the summer interns ran QA. Only offensive skills can win this game—keep your systems operational to qualify, but 0wn your adversaries to score.

Winners will be announced Sunday at DEFCON's closing ceremony.

Who is playing?
Last year's winner, Anomaly is automatically qualified to play this year's game. With the popularity of the past years games, many teams registered to play in 2004. With only seven open slots, the registered teams had to pass qualification rounds, separating the script kiddies from the truly skilled.

Teams:
1. Anomaly
2. Skewl of Rewt
3. MOCIYLB
4. Immunix
5. Enemy Combatants
6. blue9
7. Iron Grep
8. Bacon

Less formal peer groups were also visible, such as the Ethylene Crew. This was a loose association of six men and a woman that formed at Defcon 11 because of a young man who passed out in his own vomit after a night of heavy drinking. Apparently, he made quite a scene and someone wrote the chemical formula for alcohol on his forehead while he was passed out. Several attendees befriended this young man, forming a small group. They wore matching shirts with the formula for alcohol in recognition of the night that brought them together.

There was little outward evidence of stratification or leadership in peer groups like the Ethylene Crew. The same was true for more formal groups, like the Root Fu teams. The 2600 chapters were the only notable exception, based on evidence in the Defcon program. For instance, a biographical program note on a speaker named Grifter referenced his leadership role for two groups, stating he "currently runs 2600SLC, the Salt Lake City 2600 meeting, and the DC801 [Def Con Group], the Utah Defcon meeting; where he often lectures on a range of security related topics." The speaker Gene Cronk noted he was "building a successful and dynamic 2600 chapter, of which he is currently president." Another speaker wrote he was the "VP of the Jacksonville 2600." These 2600 groups demonstrate that formal hacker groups may have had a leadership structure, though it was not immediately evident to the public (see Meyer, 1989: 73). Rather, stratification was made known when those affiliated with a group specified its structure.

The generally large number of groups at Defcon may be due to its unique social nature. Since Defcon is an annual gathering with some importance in the subculture, groups may be more likely to attend as a way to learn, meet others, or participate in challenges. As there were over 5,000 people at Defcon 12, the sheer volume of attendees may have increased the likelihood of group attendance as well. Hence, Defcon may over-represent the importance of groups in hacker subculture in everyday contexts.

Hackers interviewed for this project did not commonly report membership in hacker groups. Four (30%) belonged to a group at any point in time, with 8 distinct groups described. Three of the four interviewees claimed to be involved in multiple groups over their hacking career. Three of these hackers belonged to local 2600 chapters. Membership in BBS groups was also reported, whether in cyberspace or meatspace. Finally, the hackers described belonging to private groups that were offshoots of larger associations. For example, Vile Syn participated in a programming club, which soon led to involvement in a smaller group:

Shortly after [going to the programming club meetings], we were attending private gatherings with certain members with an array of abilities. One was one of the first true hackers I had ever met, who could crack almost any software within a five-hour period of time. Another had a forte in electronics.

Indiana Tones described belonging to "a little group that was kind of on the side of 2600, but a lot of them also came from 2600." This smaller group was decidedly less organized, and more of a teen peer group as he explained:

Sometimes we'd go down to the [club] and try to pick up girls and stuff. Uh, spent a lot of time there and a lot of time in the [downtown area]. Goin' to punk shows and things like that. When we were driving around getting from place to place, man, we were always talking about the newest technology, you know, and how the rules could be bent and everything.

Membership in these groups did not mean they routinely performed group attacks. Instead, hacker groups provided contacts that facilitated information sharing. This was an important unwritten rule that many interviewees stressed, regardless of their group affiliations. Helping others learn through sharing knowledge was an important part of most relationships, and a critical normative order

(see Chapter 3 for detail). For example, Indiana Tones explained that belonging to a 2600 club increased his level of knowledge because of the members' willingness to share information:

I would help someone learn to program in visual basic if they taught me how to do web page design, you know. Or this guy here will teach this guy web page design if that guy will teach him networking. And it was basically about sharing knowledge. Not necessarily sharing, like, script kiddie attacks and things like that.

Interviewees provided little detail on the size of these groups, except for Indiana Tones who suggested the two groups he was affiliated with ranged in size from 10 and 15 members. There was also no real membership stratification. Vile Syn provided the only real evidence of leadership in any group when he described his membership in a programming club:

My father later found a local commodore club to where I could interact with other users. Of course, when we were there the first few times, I was seen as the kid the Father couldn't get away from. They had no idea that I was the user. After my father had explained to the presidents of the club that I had been coding on the Commodore, I was quickly accepted.

Likewise, there was weak evidence of any rules on relationships within or between groups. The only exception was Dark Oz who explained that in order to get onto a BBS; he had to be "hooked up" by one of his associates. He wrote "getting the Phone # to the [BBS] was hard, then they had a new user password which changed often, and then you had to get verified by an existing member or two, and verify your presence on other BBS. It was a pain."

However, the overall lack of group involvement by interviewees indicated that this was not a necessary part of the hacker experience. Some hackers felt they did not want to be affiliated with any group. Mack Diesel said, "a lot of these clubs were. . . guys out for trouble, because you know. .

. once you got into being in a club then you were more apt to be either a gray hat or a black hat."
Rather, the hackers interviewed used forums and BBS to connect with others and exchange information (see also Meyer, 1989: 63).

This may explain why eight of the hackers interviewed for this project said they almost always hacked alone (see also Meyer, 1989; Schell et al., 2002). For instance, Dark Oz wrote, "I most often work alone, but I'll discuss things with others whenever I get the chance." Two respondents suggested they hacked with others "every now and again", such as R.Shack who discussed multiple hacks with others. Kamron stated that when he hacked he was "almost never alone," and hacked with others "every month." Finally, MG gave an unclear response, suggesting he "constantly" hacked by himself and with others.[27]

However, only 10 of the 33 (30%) incidents reported by interviewees involved more than one hacker. For example, Kamron wrote that he had to "co-create a program to exploit an account privilege system" to "ruin a corrupt game server." Spuds worked with others to hack a university e-mail account system:

> We would print the list and then telnet to the machine and try the accounts and
> find the ones that had not been used an[d] then change the password to the
> password we wanted. Then we would use that account untill [sic] it was removed
> or claimed by the student.

Beyond these instances, individual hackers performed 70 percent of the hacks described. This supports the notion that "the actual performance of the phreak/hacking act is a solitary activity" (Meyer, 1989: 66). But, hackers did go to each other for advice and opinions such as Spuds who

---

[27] I was not able to reach him for clarification on this statement, and could not verify his past hacks as he answered all hacking related questions with the phrase "this is impossible for me to answer."

wrote, "I do my work alone more times than other times. It depends on the lives of those around me. I prefer to have friends around when I do my work, since there's always more than one solution."

His comments highlight an important issue regarding differences between individual and group hacks. Kamron suggested hacking with others was "a lot easier when there are a lot of steps" required to complete the hack. Multiple person hacks allowed for more creative solutions to problems and speedier attacks. Vile Syn explained, "there have been times when a few of us have done one network at once, only to cover more space in a smaller amount of time, or to do a Distributed Denial of Service (DDoS) attack." Furthermore, group hacks may be done to compete or gain some status, as Bob Jones suggested, "when we did it [hacking] it was always to see who could go the furthest. It was competition when we did it as a group."

Individual hacks were not necessarily less complicated than group hacks, since many of the interviewees felt they could accomplish most any task on their own. Dark Oz wrote, "I can do anything I set myself out to do. If I don't know how to do it, I'll teach myself. It's always been that way for me." The decision to involve others in the commission of a hack was dependent on the individual and their social network. Thus, an individual could complete the same actions a group hack required with less danger and risk to others. Vile Syn elaborated on this issue, writing:

> Most of the time I do my hacks myself. Some of my friends would like to help, but I wouldn't feel right if a simple mistake I made endangered them. There are very few [hacks] that are done with more than one person. If there are 3 people performing a chain of exploits that have to be ran in a certain time frame, things can gone [sic] wrong a lot easier due to internet lag over three different connections.

There was also little evidence that forum users hacked together. Posts in two of the six forums provided information on group based hacks, but these were mainly hacks performed by

individuals with real world relationships. For example, RatzofftoYA posted a message stating, "Me and my mates(we got a hackers team)we were expelled we install a trojan on my school's se[r]ver(we got a network) and we were having illegal access to my teachers pc, what we did was to use his connection fo[r] 2 months and his acount [sic] to get logged on to the net." In some cases, individuals with meatspace relationships used the forums to discuss their activities, as in the following post:

> **Z001@nd3r:** I personally set out on a mission to emotionally scar mine [school
>
> system administrator] if he didn't work out to scratch. He is the most pathetic
>
> excuse for a worker or admin I have ever seen, he really does do nothing but
>
> wander around, and knows only ICT [Information and Communications
>
> Technology] based stuff. After we hacked the servers at our school (me and my
>
> friend) we had made an admin account and looked through his files. We found he
>
> had loads or pro BNP material (BNP are a very racist British party) and some
>
> very disturbing images… lets just say he like Star Trek way to much (I like it, but
>
> I don't like the women in it like he did). So we emailed to all pupils in the school,
>
> everyone now knows what he spends those weekends "tuning the syst[e]m"

Such posts were relatively infrequent and did not appear in the other four forums in the data set. In fact, most of the posts on hacks involving individuals with meatspace relationships came from the forum with the largest population. Otherwise, there was little evidence to support the notion that forum users hacked together, though posters did however share information and guidance with others (see also Meyer, 1989).

As a whole, hackers formed peer groups with relatively low levels of organizational sophistication. There was little outward evidence of leadership stratification, or role specialization. These groups operated mainly to share information and facilitate learning, rather than group-based

hacking (see also Meyer, 1989: 74). This description of hacker groups was consistent with Best and Luckenbill's (1994) peer categorization, and supports the notion that "in some cases the computer underground is socially organized as peers" (Meyer, 1989: 74).

DIVISION OF LABOR

The data also provided limited support for the existence of teams based on their sophisticated division of labor. For example, the groups that participated in the Root Fu competition appeared to have some specialized roles within groups. The teams competed and worked in the open, where each person or, in some cases, pairs worked on specific components of the game. Individuals were running different programs and involved in different tasks, such as programming attack tools. The rigidity of role specialization within each team was not completely clear, but members were involved in completing specific tasks.

There was further evidence of this at the awards ceremony when the winning team was announced. The Sk3wl of R3wt won because they were able to protect their network while attacking other teams heavily. Competing teams had different strategies, and most spent time building tools to attack others. The Sk3wl of R3wt prevailed because they actively identified exploits in the system to maximize the effectiveness of their attacks. Thus, their specific strategy proved more efficient and successful.

It must be noted that the specialization observed is likely an artifact of the structure of Root Fu. The game was designed to defend a "fictional" savings bank network while attacking other systems, engaging participants in multiple roles and tasks. However, the teams clearly had some skill and understood how members needed to operate to be successful. Capture the Flag games like Root Fu reflect real world attacks and system vulnerabilities, and the game's organizers suggest it

demonstrates the ability of skilled hackers (Lemos, 2003b). So, while it is a unique event, the role

specialization and teams involved gave some insight into more sophisticated hacker groups.

There was some evidence of stratification and division of labor in the forums as well. Each

forum was a unique association composed of two distinct subgroups. One was a core group of

forum users with specific titles, such as "Administrator," "Sysop," and "Moderator" that were

responsible for rule enforcement on the forum. They monitored and deleted posts when necessary

and sanctioned users based on their actions. For example, a user made a 10-page post that was

clearly plagiarized from a book. In response, the sysops of the board made the following posts

SySop(t): It seems to me like you do not want to hear me out on the credits issue.

Your posts have been reported to the admins

and mods of each forum.

Sr. Sysop: Plagiarism is illegal and not condoned by [the forum], If your

going to copy and paste PLEASE give the proper credits to the

writer by posting the URL also.

Thread Closed

The moderator group represented a relatively small proportion of the overall user

population in each forum (see Table 4-2 for detail). For example, eight moderators posted in the

forum with 392 members; they composed two percent of the entire user population. Across all

six forums, moderators represented five percent or less of all users. There may have been more

operating on each board, but they were not present in the data.

Table 4-2: Proportion of Moderators to General Forum Population

Forum	Number of Moderators	General Population	Percentage
1	10	179	5.49%
2	1	110	.50%
3	1	20	5.00%
4	5	101	4.95%
5	2	109	1.83%
6	8	392	2.04%

The second forum subgroup comprised the larger population of users that discussed issues and exchanged information with one another. These posters provided and consumed information and, in some cases, took a role in rule enforcement. The members of this group were much more loosely affiliated with the forum than the moderators. However, there was some stratification within the user groups, via a distinct ranking system and user hierarchy. Individuals were given a rank signifying how long they had been on the forum. The labels varied across forums, and included terms like "newcomer," "newbie," or "peewee" for new users. More established users had titles like "member," "master," or "forum junkie." The ranking structures were not well explicated in most forums, however one explicitly stated the frequency of posts required for each title. As illustrated in table 4-3, the label given to a user in this forum limited the number of posts they could make during the course of a day. Newbies were limited to two posts per day, but they could become starters in two days based on the ranking criteria. Users with higher ranks had more freedom to post at any time.

Table 4-3: The User Ranking System of One Web Forum

Rank Title	Minimum Posts	Maximum Posts	Posts Per Day	Topics Per Day
Newbie	0	4	2	1
Starter	5	14	4	2
Surfer	15	24	6	3
Junior User	25	49	8	4
User	50	74	12	6
Expert User	75	99	16	8
Omnipotent User	100	124	20	10
Junior Master	125	149	24	12
Master	150	174	28	14
Expert Master	175	199	32	16
Omnipotent Master	200	224	36	18
Senior	225	249	40	20
Super Senior	250	3000	100	50

Forums also had specific written rules for all members to follow. Four of the forums had their own Frequently Asked Questions (FAQ) post or section outlining the rules for posters and moderators. One common rule across the forums was to search the board for answers to questions before posting. This was because, as one forum's FAQ stated, "the chances are good that the question you're asking today has already been answered before--- numerous times." Three of the four forums required users to respect the moderators because "showing respect is the only way to get respect." This was an important unwritten rule, since those who disrespected the moderators or their rules in any forum were subject to sanctions. The following exchange details such an instance based on Dark-ness' comments:

JoeyJoJoJuniorShabadu (Moderator): Do not post more than once in a row.

You may edit/delete previous posts by using the edit feature:

Dark-ness: JoeyJoJo, I don't think post in a row for multi [sic] times is bad.

Sometimes, when you get an idea, you post it on the board. Then anyone

who see it can have a try. Later, you find that way does not work or need

some promotion. So you can either edit your original post or add a new

one. It would cost less time to read in the first way, while the second way

provide the trace of his thoughts, which is very important in hacking. And

compared to just removing previous posts, adding new ones can tell you

that the previous way doesn't work.

JoeyJoJoJuniorShabadu (Moderator): You know what? I don't care what you think.

sAnItArIuM: Lol @ Dark-ness

Dark-ness: fuck!

sAnItArIuM: Fuck what?   Got a """"""quote""""""Strike? [a

negative mark against Dark-ness for his behaivor]""""""quote""""""

In addition, forums required users to respect each other, and avoid making flaming posts. Such

negative comments were viewed as unproductive and disrespectful:

Do not start a flame against people who you do not agree with, it is best to post

nothing at all then [sic] to flame someone. If you don't agree with a post and

want to see it closed, then send a PM [private message] to the moderator of that

forum. Flaming will get you nowhere, you will not get any respect for flaming.

The notion that moderators should handle problematic posts and users was outlined in two of

the forums' FAQs. This was an unwritten rule in forums as well, yet the general user populations

ignored this rule. For example, AtariChamp316 made a post after a well received tutorial, stating

"looks very informative but i dont feel like reading it. . . meh." Several posters who were not

moderators took the time to thank the tutorial writer while flaming AtariChamp316:

> **HackFACE:** Nice...
> Very informative, and well written. 🙂
>
> AtariChamp316: Why would you make a post that basically says nothing?
>
> **Trippledowndown:** A very well writen [sic] and informative post man… well done
> and keep it up 🙂 P.S. AtariChamp316 are you always a lazy talentless prick
> or do you just try exceptionaly [sic] hard on certain days? YOU my friend are
> whats known as a GIMP, you contribute NOTHING and post pointless posts.
> Unless you have something possative [sic] to say then say nothing at all.

Thus, the larger population of users took a role in rule enforcement, despite this being the

purview of the core group. This led to unnecessary posts and traffic that detracted from the overall

mission of the forum. Moderators attempted to control the self-help of forum users at times, as in

the following post from a forum moderator:

> I realize that many of you are dedicated to upholding the rules of [the forum], and that
>
> some of you may become annoyed when people appear to break them. I appreciate
>
> your dedication. However, arguments about whether or not a post is rule breaking, or
>
> even several posts telling the author that his post is against the rules does nothing to
>
> help the situation. The "report this post to a moderator" button is there for a reason,
>
> so please use it… If there is a dispute as to whether or not the post is actually against
>
> the rules, a moderator or admin will sort it out and take the appropriate action.
>
> Members do not need to worry about trying to do this… So, in review, when you see
>
> an illegal post, report it.

Written and unwritten rules were also prevalent at Defcon, though they were distinct from rules in the forums. For example, there were clearly written rules for the teams participating in games at Defcon that varied with each specific event. Figure 4-2 details the rules of three of the mini-games of the wardriving competition. Each of these mini-games had its own set of rules dependent upon the objectives of the game. The Running Man and Tag games required no more than two players per team, while the Fox and Hound limited teams to "the total number of people who can safely sit in a single vehicle."

Figure 4-2: Wardriving Mini-Game Rules

FOX AND HOUND

Object: Be the first team to locate the "Fox."

Sponsored by NetStumbler.org (www.netstumbler.org) and Michigan Wireless (www.michiganwireless.org)

Date/Time: Saturday, July 31, 18:00-21:00
• Time limit of 3 hours.
• Teams must be at least two people (driver & RF person/navigator) and limited to the total number of people who can safely sit in a single vehicle.
• No multiple vehicle teams.

RUNNING MAN

Object: Be the first to locate and id the "Running Man."

Sponsored by Blackthorn Systems (www.blackthornsystems.com)

Date/Time: Saturday, July 31, 13:00-14:00
• Time limit of 1 hour.
• Limited to single players or two-person teams.
• Two person teams must work together, no splitting up allowed.
• Players should realize that this is DEFCON, and than means within 5 minutes of the contest's start approximately 492 spoofed RunningMan web servers will exist. The organizers cannot control this, so don't even bother to ask. Besides, it will add to the challenge. You don't want it to be TOO easy, did you?

TAG (YOU'RE IT!)

Object: The goal is to place a text file (yourname.txt) in a shared directory of a particular machine. The first one that does wins. The text file must be in the format listed below and have your PGP public key so that we may confirm the winner.

Sponsored by FAB-Corp (www.fab-corp.com)

Date/Time: Friday July 30, 18:00-21:00
• Time limit of 3 hours.
• Limited to single players or two-person teams.
• The name and public PGP key of each player must be submitted before the start of the contest. (Two man teams may choose one team member's PGP key.)
• Two person teams must work together, no splitting up allowed.
• Once again, players should realize that this is DEFCON, and than means within 5 minutes of the contest's start approximately 8.6 million spoofed TAG servers will exist. The organizers cannot control this, so don't even bother to ask. Once again, it will add to the challenge.

There were no specific written rules governing the relationships or conduct between groups at Defcon, though some informal rules were evident for all attendees. For example, people were to have fun at Defcon. The convention organizers referred to Defcon as a party, and the attendees I spoke with came to have a good time, as well as learn. The various interactive games, parties, and the on-site rave reinforced this notion. Another unwritten rule was to not use the hotel's Internet access. The wired and wireless networks in the hotel were constantly being monitored or "sniffed" by attendees seeking to highlight the weaknesses of computer security products. If a user who logged on did not have any real time security or encryption tools, then their information would be obtained and posted on the "Wall of Sheep" or "Wall of Shame."

Figure 4-3 provides an image of the "Wall," which consisted of a projector running the username, password, and other information of those who were on the network at any given time. This served as a unique source of both embarrassment and education, since only those with weak system security would have their personal information posted. For instance, one individual with no real security software filed their taxes through the hotel's Internet connection. This traffic was discovered, and a message was posted on the "Wall" stating "DON'T DOWNLOAD YOUR TAX RETURN @ DEFCON" (Cheung, 2004). This unwritten rule played an important role in demonstrating the value of secure Internet use for Defcon attendees.

Figure 4-3: Wall of Shame/Sheep Screen (from Cheung, 2004)
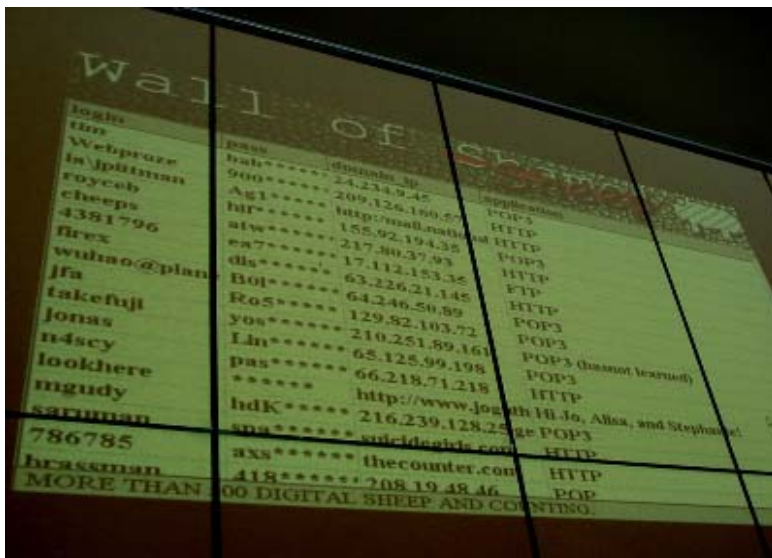
Attendees were also encouraged to share information with others and help them learn. This was one of the primary objectives of the convention, and individuals had multiple opportunities to share files and information. In turn, attendees could form social relationships through these interactions. The convention organizers were hopeful that individuals could make such connections, writing: "The Con is what you make of it. Do not be afraid to introduce yourself to others, or to ask questions of the speakers. We have provided you with a canvas, it is now in your hands to fill in." Thus, learning and forming relationships played an important role in the Defcon experience.

Generally, there was limited evidence of hacker teams, or at least within the Best and Luckenbill (1994) framework. A small number of groups at Defcon had clear divisions of labor, specialized roles, and operated to achieve a specific goal: win a competition. The moderator groups of forums also fit within the ideal team category since they were small, had specialized roles, and rules on behavior. At the same time, there was no evidence that they hacked in groups. The larger group of users seemed to constitute colleagues, or peers, because of the relationships between individuals that were used to exchange information, and occasional mutual participation in hacking. However, the forums as a whole did not constitute teams.

EXTENDED DURATION

The final element of organizational sophistication to be considered is extended duration. Across all of the data, there was no clear evidence of any group with an extensive history. Most relationships and groups appeared transitory, particularly with regard to the forums. In fact, three of the six used for this research no longer exist. Two of the groups no longer support forums on their websites, and the entire site for the third forum was taken down. This is especially remarkable as this third forum billed itself as the largest on-line hacker community. Similarly, Meyer (1989: 41)

found the lifespans of the BBS he studied to be relatively short, ranging from one month to one and a half years. Thus, the forums appeared to be relatively transitory groups.

In turn, relationships within forums were somewhat weak and short-lived. Consider that most users posted less than three times in each forum. There was no guarantee that an individual used a specific forum every day. Drains on users' time may keep them from actively participating in a forum, as exemplified in this exchange:

Sazzazza: i have twice msg [messaged] cr@ckh3@d according to his commitment.

but he dosnt [sic] respond [to] any one of them so here i m again..want to

know what is CGI server..?

all replies would be appreciated.

Thanks!

cr@ckh3@d: well just came online and saw your msgs [messages]...

for your information Sazzazza...some people have to work during

the day and cant be online every single day.....

so dont expect to get a reply as soon if someone msgs me...

In another forum a newsletter was supposed to be sent to members, but it had not been done in some time. The following exchange detailed why this lapse occurred:

Cyrus: Newsletter?

Wot [sic] newsletter, out of all the time ive [sic] been registers I havent

received a newsletter. Surely someone can make one?

PhallaCY: As of now, no future newsletters are in the works. Not many people

have the time to keep it up.

665: Mabey [sic] we should get people who have the time to make it up?

Calculonicon: well, if you want to do it, then by al[l] means, submit work and

get people together

All of the people who had the time and interest to do the newletter

[sic] before have parted, so we need new people

There was no real evidence of purposive relationships between forum users either. Instances of hacks performed by members across forums were not found. Examples of group hacks were in the data, though there was nothing to suggest they involved users from different forums. It is possible this does happen, as individuals belonged to multiple forums at once, but this possibility was not evident in the data. There was also no indication of meetings between forums. Users had some knowledge of other forums, and used them because of specialized content or knowledgeable members. However, there was no evidence of interactions between core members of different forums. Thus, relationships between forums appeared to be based on weak, loose affiliations.

None of the hackers interviewed for this project provided information on the duration of groups over time. There was no information on the lifespan of the groups involved with Defcon. Yet the fact that the convention is in its twelfth year is worth noting. Defcon has become the oldest hacker convention in the US, and an important part of the hacker subculture. Long-standing groups like the Cult of the Dead Cow have used Defcon as a launch party for different security/hacking tools (see Furnell, 2002). Hence the convention, its organizational hierarchy, and communal atmosphere has persisted.

Furthermore, Defcon provided some evidence of multiple purposive relationships between groups. Several different organizations worked together to promote or sponsor events. For example, members of Defcon Group 801 and Rootcompromise.org organized the Defcon movie channel efforts. The Scavenger Hunt was organized and sponsored by the slc2600 and Rootcompromise.org.

Netstumbler.org and Michigan Wireless sponsored the wardriving mini-game Fox and Hound. In addition, individuals from some of the Root Fu teams also sat together during the awards ceremony.

Defcon also demonstrated purposive relationships between individuals. Defcon provided an opportunity for individuals to connect with one another in the real world. Attendees were able to share information and have fun, which was key for those with on-line relationships. For example, I spoke with three attendees who knew each other through their use of Defcon forums. They conversed regularly through web forums, but used the convention as a way to foster their social relationships. These individuals came from areas where there was no real hacker "scene," which led them to develop social networks on-line. Individuals could expand their network by meeting others during the course of the convention. The convention organizers have recognized this fact, and developed ride and room sharing programs to help increase attendance and create social connections (Defcon, 2005b). Thus, there were multiple opportunities for hackers to expand their relationship networks at Defcon.

Taken as a whole, there were no real deviant formal organizations within the data. Best and Luckenbill (1994) define deviant organizations as organizations that are involved in deviance (p. 72). However, the Defcon organization was not openly or outwardly involved in deviance. Instead, information was given to facilitate deviant behavior but Defcon did not support deviant behavior. Furthermore, the convention organizers did not condone any sort of illegal hacking or otherwise criminal behavior. Defcon's private security "goons," and local law enforcement were on hand to ensure that individuals did not engage in such activities. This key issue is what may make Defcon a legitimate, rather than deviant, formal organization.

CONCLUSION

In sum, these analyses clearly indicated that hackers are not loners (see Meyer, 1989). They created social networks with other hackers in the real world and cyberspace, and operated within a subculture emphasizing unique normative orders, including knowledge and learning. The on and off-line social ties between hackers facilitated information sharing and introduced subcultural normative orders to new hackers. However, the act of hacking was an overwhelmingly solitary behavior, regardless of an individual's social ties. As Meyer (1989) found 16 years ago, it appears that hackers still constitute colleagues according to the Best and Luckenbill (1994) framework.

There was also evidence that hackers belonged to groups of various sizes with little stratification or role specialization. Membership in these groups was not heavily reported, and there was weak supporting evidence that they performed group-based hacks. Instead, these groups facilitated hacking by providing individuals with information and resources. This is an important point, as mutual participation in deviance is one of the key requirements of the peer category (Best and Luckenbill, 1994). But groups created and fostered relationships between individuals that facilitated information sharing. This suggests there are peer groups within the hacker subculture, though they are not very sophisticated (see also Meyer, 1989).

Groups with specialized roles and divisions of labor when hacking were present in the Defcon data, but only in limited numbers. The small groups of forum moderators could also constitute teams based on their clear division of labor, stratification, and rules on the behavior of members. At the same time, members of the broader user group were loosely tied to each other and did not offend as a collective. Thus, forums as a whole did not clearly fit within the continuum of organizational sophistication.

There were similar complications regarding the Defcon convention as a whole. The convention could not operate without the cooperation of multiple groups to sponsor and organize the various events. Roles were coordinated in advance, ranging from security "goons" to speakers. There were specific rules on the behavior of attendees, and almost 5,000 people present at the convention. Defcon has become the longest operating hacker convention in the U.S. and an important part of the subculture. As such, it may constitute a formal organization because it has all the characteristics of organizational sophistication including extended duration across time and space and purposive relationships between groups. But it is most likely a legitimate formal organization because of the convention organizers' insistence that they do not support deviant or criminal behavior.

Hackers were arrayed along the continuum of deviant and non-deviant organizational sophistication. This was a considerable shift from Meyer's (1989) finding that "there is no evidence to support assertions that the CU [Computer Underground] is expanding" and "is not likely to do so on a large scale" (p. 80). In fact, hackers may now constitute a community which Best and Luckenbill (1994) define as "groups which share a common territory and a higher degree of institutional completeness" (Best and Luckenbill, 1994: 68). This is a unique and more sophisticated form of organization that Best and Luckenbill (1994) discuss, but do not include in their framework. They excluded communities because they are relatively rare and do not often develop, due to the increased presence and penetration of law enforcement in modern society (Best and Luckenbill, 1994: 72).

However, there is evidence that hackers have the defining characteristics of a community, including their use of common territories. Hackers did not necessarily share common territory in meatspace, as they had relatively small peer groups and limited involvement in hacker groups. But,

web forums, e-mail, and other forms of computer mediated communication allowed hackers to develop shared on-line spaces. Many of the hackers interviewed for this project used on-line resources and forums to make contact with others and share information. Conventions like Defcon could constitute a sort of shared space, providing a location for individuals across the country or globe to come together in one place to discuss issues and socialize. So, while hackers do not have a specific territory in a traditional sense, they have spaces that allow them to connect with other hackers.

Communities are also "institutionally complete," meaning that they have institutions that serve the interests of their members (Best and Luckenbill, 1994: 68). A variety of groups, businesses, and conventions cater to hackers, from clothing companies like JINX Hackwear, to magazines such as the 2600 and Blacklisted. An inordinate number of web forums exist providing social links to other hackers, as well as resources to hack. Real world hacker groups and conventions operate across the globe to foster and develop interest in hacking and technology. Legal rights groups like the Electronic Freedom Foundation also serve the interests of hackers and the larger digital world. In addition, hackers have banded together to generate social support and legal funds, as in the case of the famous hacker Kevin Mitnick (see Loper, 2000). Thus, hackers appear to be institutionally complete because of the multitude of institutions providing goods and services for hackers.

Furthermore, Best and Luckenbill (1994) suggest communities form in two ways. The first method is in isolation where social control agents may have difficulty accessing or interrupting deviance (Best and Luckenbill, 1994: 71). The early use of Bulletin Board Systems and the Internet by computer hackers isolated their behavior to some extent, requiring individuals to have a firm grasp of computer technology to access these materials. But the subsequent growth and ubiquity of computer technology has made the Internet a global phenomenon. Instead, a hacker community may

be forming through a second way: through a decline in law enforcement efforts as a deviant act becomes legitimized (Best and Luckenbill, 1994: 71).

While hacking is an illegal act that can lead to arrest and prosecution, there is some indication that hackers are becoming involved in legitimate activities. The presence of government and business representatives at Defcon attempting to recruit individuals for employment reflects the legitimization of hacking. The number of interviewees who worked in computer security and information technology positions also echoes this notion. Connections between Defcon and the Black Hat computer security conference, as described in Chapter Three, highlight the increasing legitimization of hacking as well. Thus, there is some evidence that the deviant nature of hacking is changing. If this trend of legitimacy continues, this may provide further validation for the existence of a hacker community.

On the other hand, it is clear that hackers continue to operate primarily as colleagues, peers, and in some cases, teams. This is very similar to Meyer's (1989) findings on hacker social organization 16 years ago. Nonetheless, my findings suggest that legitimate formal organizations like Defcon now exist. Likewise, evidence that hackers may now operate as a community is an advancement, which emerged specifically through my examination of both the social organization and subculture of hackers in tandem. Such an analysis can elaborate the ties between social norms and values and the ways that individuals form relationships with others. However, the relationships between these two constructs and behavior must be considered as well. The connections between hacker subculture, social organization, and behavior are more fully explored in the final chapter.

CHAPTER FIVE: SUBCULTURE, SOCIAL ORGANIZATION, AND DEVIANCE

This dissertation has explored the normative orders of computer hacker subculture and its social organization using three qualitative data sets. Chapter Three considered the five normative orders of hacker subculture, and the way they shape individual behavior. I investigated hacker social organization in Chapter Four using concepts derived from Best and Luckenbill (1994) and Decker et al. (1998). This examination demonstrated how hackers operate in individual and group contexts.

Research on these two facets of social relationships provides insight into the way that both the subculture and social organization of criminals affect behavior. The social organization and normative orders of a deviant subculture also have reciprocal influences on one another. In addition, there may be some instances in which the nature of the deviant act itself plays a role in shaping subculture and social organization. The interconnections between subculture, social organization, and behavior are rarely examined in tandem, limiting our knowledge of the way each shapes the other. There may be more complex relationships present that have not been fully articulated, and we do not know how consistent they are across crime types. In this final chapter, I attempt to explore the relationships present between the organizational practices of hackers, normative orders of hacker subculture, and hacker behavior. This analysis will expand our knowledge of how these factors shape one another.

To accomplish this, I compare the results of my examinations of hacking, hacker subculture, and social organization with evidence from sociological research on the way that subculture and social organization shape behavior. Specifically, I assess the consequences of hacking, hacker subculture, and social organization on the enculturation of hackers and their ability to complete complex hacks (Best and Luckenbill, 1994: 77). I also consider how social organization, subculture, and the nature of hacking impact social control agents' attempts to locate, apprehend, and sanction

hackers (Best and Luckenbill, 1994: 88). Finally, I examine how these three elements affect hacker careers, rewards from hacking, and responses to social control efforts (Best and Luckenbill, 1994). Instances where my findings support or contradict known relationships will be identified and explored in detail. Following this analysis, I review the overall findings of this dissertation. I then conclude by considering the implications of this study for policy making and future research.

Consequences of Social Organization, Subculture, and Behavior

Examining the way that hacker subculture, social organization, and behavior influence one another revealed a number of relationships. To begin, the social organizational and subculture of hackers have important consequences for hackers' ability to complete complex hacks. Research suggests that the organizational sophistication of deviants affects their ability to perform elaborate and complicated criminal acts (Best and Luckenbill. 1994: 77). The more organized a group, the more intricate their activities can be. However, this is tempered by deviants' access to resources, which facilitate the commission of deviant behavior (Best and Luckenbill, 1994: 77). It appears that those who have greater access to resources can perform more complex crimes regardless of organizational sophistication. Thus, availability of resources has a significant impact on the ability of deviants over and above their level of organizational sophistication.

This may explain why hackers, who most often offend alone, are able to complete complex hacks. Recall that hackers in this study primarily operated as colleagues, meaning that they had relationships with other hackers and created a subculture, but largely hacked alone. There were also a number of peer groups present, where individuals occasionally hacked with others. These relationships allowed hackers to gain access to resources in myriad ways. Hackers used their connections to other hackers to exchange information, ideas, and materials on and off-line. Even the

relatively weak relationships between forum users, for instance, provided hackers with knowledge that could be used to facilitate hacks.

The hackers' collegial and peer networks were also couched in a much more sophisticated, but just as loosely connected, form of organization: the hacker community. This community exists because hackers have shared spaces and are institutionally complete, as myriad resources in both cyberspace and meatspace serve the interests of hackers and facilitate hacks. For instance, hacker groups like the 2600 and Defcon groups provide hackers with materials, information, and social relationships. Hacker web sites like Bugtraq provide hackers with information on the latest exploits in systems. Forums also give access to materials and social relationships with others. This demonstrates the significant impact resource availability has on deviant behavior, regardless of organizational sophistication (see Best and Luckenbill, 1994: 77).

The normative orders of hacker subculture reinforced the ability of hackers to complete sophisticated hacks. Hacker subculture placed significant value on individuals developing a strong body of knowledge that could be applied to hacking. Exchanging new or useful information with other hackers was an important way to increase knowledge and gain status. The normative order commitment also stressed the amount of time hackers should spend reading and gaining hands-on experience with computers on their own. This improved the individual hacker's ability to hack, in addition to the level of respect they were shown by others. Hacker subculture supported the ability of hackers to perform complex hacks on their own by structuring hacker behavior to provide access to resources and articulating the importance of individual knowledge. Thus subcultural norms reinforced the importance of individual knowledge and ability, and supported the idea that hackers need not operate in groups to successfully perform challenging hacks.

At the same time, the act of hacking may have an impact on both hacker subculture and social organization. Technological innovations have simplified the act of hacking and increased the ability of hackers to complete complex hacks. The development of the World Wide Web and user-friendly attack programs, or scripts, allow individuals without sound technological knowledge to hack. Anyone can download the tools to engage in behaviors that previously required some skill. For example, the remote administration tool Sub7 allows an individual to take control of another person's system. In turn, would-be hackers do not need to belong to formal or even informal groups to perform complex hacks. They only need to gain access to the tools via websites and other on-line resources, which can be easily identified through web search engines. Thus, innovations in technology and hacking may influence hacker social organization by reducing the need for strong social relationships or involvement in organizationally sophisticated groups.

While the ability of individuals to complete complex hacks with ease reinforces the collegial nature of hacker social organization, it has a different influence on hacker subculture. The act of hacking appears to affect the way hackers relate to one another within hacker subculture. Specifically, the hacker argot recognizes the increasing number of unskilled hackers who can easily complete hacks with devastating consequences. Derogatory labels like script kiddie are applied to those who hack but do not fully understand the technology they use. Script users are given little status because hacker subculture places tremendous value on understanding technology and learning to hack. Hackers do not treat those who use such tools in the same way they would a knowledgeable hacker. Thus changes in hacking affect the relationships between hackers by differentiating between hackers based on their knowledge, as well as their ability to hack. This is an important relationship that demonstrates the significant impact that behavior can have on the nature of subculture and social organization.

In addition, subculture, social organization, and behavior influence the enculturation of deviants. Research indicates that social organization influences deviant enculturation, as greater levels of organizational sophistication lead to more elaborate deviant enculturation (Best and Luckenbill, 1994: 78). For example, Best and Luckenbill (1994) suggest loners do not receive any sort of instruction from others to engage in criminal behavior. On the other hand, newcomers to more sophisticated organizations such as teams receive far more complex training, including apprenticeships with experienced criminals (see Chambliss, 1972). The hackers in this study have collegial relationships, and were introduced to subcultural norms and values through their connections with others. The transmission of subcultural knowledge occurred both on and off-line, and was apparent across the data sets. Nonetheless, hackers were not actually taught how to hack by others. They may have obtained pieces of information and advice from others, yet no one in any data set indicated that another hacker formally trained them. This provides some support for the notion that the enculturation of deviant colleagues is much more limited when compared to more elaborate forms of organization (Best and Luckenbill, 1994: 78).

The enculturation process of more sophisticated hacker groups appeared limited as well. For example, the hacker teams present at Defcon had no apparent or specific regulations on member behavior. This may be a result of my limited access to these groups. But even the codified and informal rules evident in the forums did not apply outside of their boundaries. This indicates that hacker groups are less organizationally sophisticated compared to other criminal teams and formal organizations which have intricate codes of conduct with binding rules on relationships at all times (see Wolf, 1991). Moreover, this demonstrates the weakness of hacker enculturation.

The act of hacking may also play a role in limiting hacker enculturation because a hack does not typically require multiple participants to be completed. There was little evidence that forum

users hacked together. Most of the hacks reported by interviewees involved a single person as well. In fact, the hackers interviewed for this research suggested that a hack could be performed with or without the immediate assistance of others. Rather, the decision to work with others was contingent on the individual hacker and his social network. Thus, the nature of hacking reinforces loosely coupled hacker social organization practices by not necessitating deep relationships with others.

Consequently, hacker social organization and the act of hacking may have had a destabilizing influence on the normative orders of hacker subculture. Many hackers and forum users recognized the value and importance of a broad understanding of technology, but indicated there was no one way to become a hacker. The normative order classifications demonstrated that hacker identity was heavily influenced by personal opinion. Individuals had different opinions regarding what constitutes a hacker, ranging from the ability to perform certain tasks to the acceptance of specific attitudes. Hacker identity appeared to vary from person to person based on their beliefs about hacking, rather than group consensus.

This suggests that social organization and behavior influence the structure and acceptance of the normative orders of hacker subculture. Few researchers have considered such a relationship, particularly with regard to the relationship between deviant acts and actors. Though there is no clear way to determine the causal order of this relationship, it does present a potential refinement of our understanding of the influence of social organization and behavior on the structure and enactment of subcultural norms.

Law Enforcement Efforts To Stop Hackers

Subculture, social organization, and the act of hacking not only impact hackers, but the activities of law enforcement as well. Researchers suggest that law enforcement must tailor their enforcement strategies depending on a deviant group's level of organizational sophistication (see

Best and Luckenbill 1994: 88). Greater resources must be expended to deal with more sophisticated groups, while less effort is required to deal with lone deviants. Furthermore, subcultures can provide deviants with ways to rationalize their actions, and conceal themselves from policing agencies (Sykes and Matza, 1957). This suggests social organization and subculture affect the activities of social control agents.

My findings indicate that hackers pose a unique challenge for law enforcement since they operate at different levels of organizational sophistication. Hackers function both as individuals and groups, and also exist within a larger community. Hacker subculture recognizes the threat of law enforcement, providing rationalizations for behavior and creating an undercurrent of mistrust between hackers and policing agencies. This was evident in the normative order law (see also Taylor, 1999). Moreover, the interviewees and forum users noted that the act of hacking can be technologically sophisticated, allowing skilled hackers to obfuscate their identity or activities (see also Wall, 2001; Grabowski and Smith, 2001). As a result, there are myriad complications law enforcement must face when dealing with hackers.

The larger literature on hackers indicates that a number of strategies have been devised by law enforcement agencies to access and arrest hackers. Many of these efforts mirror those used to break up different types of organized crime (see Abadinski, 1990). For instance, specialized federal task forces, such as the Federal Bureau of Investigation's Computer Hacking and Intellectual Property (CHIPs) units, have been developed to deal with hackers and other computer criminals (Department of Justice, 2002a). Computer forensics units have also been created to obtain evidence from seized computers and aid in the prosecution of hackers (see Noblett et al., 2000). Furthermore, large scale crackdowns, such as Operation Sundevil (see Sterling, 1992) and Operation Buccaneer (Department of Justice, 2002b) have been implemented to arrest hackers across the country.

In addition, my findings provided evidence that policing agencies utilize extraordinary steps to deal with hackers, including observing their activities on and off-line. Law enforcement agencies have used hacker conventions like Defcon as a way to observe hacker activities in meatspace (see also Sterling, 1992). The variety and number of law enforcement agents at Defcon 12 were quite obvious, due in large part to hackers' efforts to publicly identify federal agents. Surveillance efforts are also being used in cyberspace, as with the National Security Agency's ECHELON program that can monitor and scan network traffic for the presence of certain words or terms (see Hamelink, 2000). Several forum users and interviewees noted the increasing threat of electronic eavesdropping and expressed concern regarding the monitoring of web forum traffic and posts between individuals.

Partnerships are developing between policing agencies and businesses to identify and arrest hackers as well. For instance, Microsoft, the FBI, and Interpol have begun to work together to offer rewards for information leading to the arrest of virus writers and hackers (Lemos, 2003). I found similar relationships between hackers, businesses, and the law enforcement community across the data. For instance, hackers asked about employment with the FBI and other agencies during the "Meet the Fed" panel at Defcon. Many of the hackers interviewed for this research work in computer security jobs. Even well known criminal hackers like Kevin Mitnick have formed security companies to deal with hacking and other computer based threats to businesses (Mitnick Security Consulting, LLC, 2005).

While the security community has debated the true value of working with hackers (see Taylor, 1999; Schell et al., 2002 for discussion), these arrangements provide some immediate benefits for both the business and law enforcement community. Hackers can provide an insider's perspective on how and why people hack (Taylor, 1999). They make excellent computer security practitioners because they can apply their skills and knowledge to defend against outside attacks, as

many of the individuals interviewed for this research suggested (see also Taylor, 1999: 96). Hackers also recognize the value of understanding computer technology at deep levels, and endeavor to constantly improve their skills. Thus law enforcement agencies and businesses that partner with hackers benefit from subcultural values like commitment and knowledge. This provides support for the notion that hacker subculture, social organization, and the act of hacking affect law enforcement strategies to detect and arrest hackers (see Best and Luckenbill, 1994; Sykes and Matza, 1957).

Hacker Responses to Law Enforcement

In response to these detection and enforcement strategies, hackers have taken steps to conceal their activities from law enforcement. There was relatively limited evidence in my data that the act of hacking provided significant protections for hackers above and beyond their ability to conceal their actions. However, research suggests that social organization practices can reduce the threat of law enforcement. Sociologists assume that at lower levels of organizational sophistication, criminals are much less secure from social control agencies because there are fewer mechanisms in place to protect individual actors (Best and Luckenbill, 1994: 86). For example, formal organizations may have attorneys available to assist criminals, whereas loners have little to no such resources (see Cressey, 1969; Best and Luckenbill, 1994).

Yet I found evidence of informal protections for hackers in their collegial and peer relationships. The loosely connected social networks between hackers provide some insulation for their activities. Individuals with on-line connections may know very little about the personal lives of their associates, reducing the level of information that could be used against them later. Interviewees often emphasized this point, stating they knew very little about the individuals that they met on-line. Hackers' use of handles or nicknames also functions to conceal their identities (see also Thomas, 2002). Very few individuals used their real names when posting in forums, and some Defcon

presenters used nicknames or pseudonyms despite the fact that the convention took place in

meatspace. This practice is beneficial in reducing the level of intimate knowledge hackers have of

each other, and contradicts the notion that limited protections are in place within collegial and peer

groups (Best and Luckenbill, 1994: 86).

My findings also indicate that the larger hacker community, both on and off-line, affords

hackers greater cover from policing agencies by providing access to different resources. Legal rights

coalitions like the EFF give specialized legal protection for the rights and interests of hackers. Hacker

publications provide information on how to secure their activities from law enforcement. For

example, a treatise was printed in the Defcon program on how to reduce law enforcement detection.[28]

Figure 5-1 provides a portion of this document, detailing the actions hackers should take to reduce the

potential for law enforcement detection, including the use of encryption software and understanding

what laws may be violated by hacking. Thus, the protections afforded by the hacker community

augment the informal measures used by hackers in their immediate relationship networks.

Figure 5-1: Notes On Avoiding Law Enforcement Detection From the Defcon 12 Program

this.

Many years ago, I was talking to Mind Rape on the phone, and he said (I'll paraphrase) "they're all out to get me, they're tapping my phone, they're watching my every move". He turned out to be correct, I thought he was wrong at the time, but being right was useless—he still got busted.

THINGS TO AVOID

Lets talk about things to avoid. Many of these are obvious.

Don't write things down. Little scraps of paper is probably the reason it takes the government 4 years to prosecute a person after they've been raided. But they do prosecute. Think of your output in terms of 'evidence'. Try to create as little of it as possible.

This includes a notebook! How to operate away from your house? Make a printout and burn it when your done. Realize that cops can trash just as easily as we can.

Gail Thackery and her ilk love our tradition of having a notebook that's rich in diverse information. Don't make their jobs any easier than you have to.

Use encryption. Encrypt everything. Make it easy (so you do it!), but don't compromise your security. Using all the encryption in the world doesn't help if you have a 'bust-me notebook'.

If people you know get busted, lay low for awhile. Be aware that the police probably have your number if he called you direct.

You shouldn't have to 'clean house', or go on an evidence destroying purge, because you shouldn't generate much evidence. System logs should be considered evidence as well.

If you have reason to believe you are going to be busted move your system elsewhere. Store your encrypted data someplace very safe (not where the system is located). When loaning out your computer, wipe (and government standard wipe!) your drive free of all data. Norton has a good wipe utility.

If you do most of your hacking from your own account, there's nothing I can say to make you smarter. Ditto with the home phone and phreaking.

Know the laws. Don't rely on hacker folklore. No matter how long your "really, I'm not a fed" BBS application is it won't protect you. It may in fact call attention to you, or confirm your illegal intents. Read the laws. Go to resources that are somewhat reliable. Don't expect your case to be a cause.

Know what crimes you're committing. Know the penalties. Know the jurisdiction (it could be FBI, SS, Local, State, or international authorities).

If you can, know the policies of your victims. For instance many people won't pirate Novell because of their Draconian tactics against BBS's who carry their warez. Many companies won't prosecute hackers because of their fear of loss of public trust and stockholder reactions. Many or most law enforcement investigations (concerning corporate hacks) start out because a company files a complaint. If they refuse to file complaints then they are much safer to penetrate.

Note that many corporate security officials have close ties with law enforcement. One day after a friendly informational interview with Microsoft Piracy investigator I received an email from a friend of Gail Thackery telling me to call her. This is a 'web' of enforcement, coordinated in many cases. Be aware of this, don't write off the person whose job it may be to find you. You don't ever want that attention, best if they never knew you were there.

There is a risk to everything we do in life. This is often part of the reason why we do it. Don't be scared, be informed and cautious— and hack, phreak, or pirate free from paranoia.

---

[28] This originally appeared in the Defcon 3 program, but was reprinted because its author, Dead Addict, felt it still provided valuable information for today's hackers. Also, Gail Thackery is mentioned because she has prosecuted several hackers and is well known in hacker subculture.

Hacker subculture provides some protection from the threat of legal sanctions as well. This was evident in the normative orders of hacker subculture that reinforced the importance of concealing hacks from law enforcement. The normative order law stressed the need for hackers to understand the law. Hackers in the forums frequently discussed the legal nature of certain hacks and related activities, and whether they should be performed. The threat of law enforcement was prevalent in the subculture and affected hacker behavior at Defcon and in the forums. Hackers placed value on concealing criminal hacks from others, and rationalized sharing information with potentially illegal applications as a way to educate others. Even the hacker argot differentiated between criminal and non-criminal hackers through the use of the term "cracker" and "hacker." A similar linguistic separation to describe hacker activities was evident in the use of "whitehat" and "blackhat". Thus, subcultural norms were enacted in response to the threat of social control agencies, in a similar fashion to the efforts taken by hackers in their collegial and peer networks. As a result, hacker subculture and social organization may structure the nature of hacker behavior to reduce potential threats posed by law enforcement.

Hacker Careers

However, the relationships between subculture, social organization and behavior were less clear when considering hacker careers. Research posits that deviant careers are influenced in part by social organization and subcultural norms. For instance, Best and Luckenbill (1994) suggest that the organizational sophistication of a group affects the duration and intensity of deviant careers (p. 83). Criminals involved in more sophisticated teams and formal organizations tend to devote more time to their deviant careers, while loners and colleagues have less time to spend involved in deviance.

My findings contradict this notion, as most of the hackers invested a significant amount of time hacking and learning about computers and technology, despite relatively low involvement in

sophisticated organizations. Specifically, while hackers were primarily involved in collegial and peer networks, the larger hacker community had a more significant impact on hacker careers. This was due largely to the resources available through this community that easily connect hackers to other hackers and hacker subculture. For example, on-line forums connect hackers to discuss a myriad of technical issues or simply to relate to others with an interest in computers. Hacker conventions immerse individuals in hacker culture for a few days each year. Thus, long term involvement in hacking is facilitated by remote access to resources, especially through the Internet. This suggests that resource availability shapes the ability of hackers to complete deviant acts and may also affect the length of deviant careers.

In addition, research indicates that the internalization of a deviant identity affects the length of deviant careers. It is argued that the more an individual accepts a deviant identity, the longer they will persist in deviance (Best and Luckenbill, 1994: 84). Social organization research suggests that at greater levels of organization, individuals are much more likely to accept a deviant identity because they spend larger amounts of time around deviant individuals. However, subcultures appear to have a much more significant affect on the development and acceptance of deviant identities. Subcultures provide values and beliefs that structure attitudes toward deviance and influence behavior (Miller, 1958; Short and Strodtbeck, 1965). The enactment of such behavior influences the way that an individual is viewed by others, and in turn, themselves (Blumer, 1969).

The relationship between behavior and identity construction was evident within the normative orders of hacker subculture. Hacker subculture placed strong emphasis on the constant development of skill and knowledge, as identified in the order commitment. In turn, the hacker argot was structured around an individual's commitment to hacking and their connection to technology. For instance, skilled hackers who used their knowledge to perform malicious hacks

were often referred to as black hats. Individuals who were not willing to put the time and effort forth to learn to hack were shown little respect and given derogatory labels like script kiddie. Thus, the application of these labels played a role in the development and construction of hacker identity.

At the same time, hackers may not fully accept a deviant identity based on the role of personal opinion in the construction of hacker identity. Some individuals did not view hacking as a harmful activity and suggested that certain types of hacks should not be illegal. Hackers differentiated themselves from criminal hackers through the use of the term "cracker." Furthermore, some felt "hacker" was an ideal term that could only be aspired to, due to the level of knowledge a "hacker" must have.

This differentiation in identity was also evident in comments from interviewees with jobs in computer security and IT who felt they were different from deviant or criminal hackers (see also Jordan and Taylor, 1998; Taylor, 1999). These individuals were no longer involved in deviance or felt no desire to perform illegal hacks, yet viewed themselves as hackers based on their level of knowledge and ability. A hacker's acceptance of deviant identity may vary due to the individual construction of hacker identity espoused by hacker subculture. The relatively limited enculturation process of hacker subculture leads to a lack of consensus on the meaning of the term hacker, as well as the other labels within hacker subculture. Thus, hacker subculture affects the acceptance of deviant identities through the development of individual meanings for behavior which may or may not view hacking as a deviant behavior.

At the same time, the act of hacking also structures deviant identity, largely because individuals can hack without violating the law. Some interviewees engaged in penetration testing on their home networks and those of other businesses for a living. These tests involved hacking, but were legal activities. Others collected information that could be used to facilitate hacks, but did not

apply their knowledge in illicit ways. For example, Dark Oz developed a collection of viruses and occasionally unleashed them on his system to understand how they operate. This is completely legal, as he never sent a virus to others. Therefore an individual can become a hacker without actually violating the law, which most likely reduces the development or acceptance of a deviant identity. This suggests that hacker identity is influenced in part by the activities an individual engages in, as well as their personal conceptions of hacking. Thus, the act of hacking and hacker subculture may have contradictory affects on the length of criminal hacker careers, given the range of deviant and non-deviant identities available to individuals within the subculture.

Rewards From Hacking

Research suggests an important factor in shaping the length of deviant careers is the rewards individuals derive from offending, including money and emotional affects (see McCarthy and Hagan, 2001; Wood et al., 1997). Individuals will continue to offend as long as the benefits experienced are greater than those produced by engaging in other activities (Matsueda et al. 1992; Best and Luckenbill, 1994). Researchers also argue that organized groups can experience more consistent benefits over long periods of time due to their ability to regularly offend (see Best and Luckenbill, 1994: 84; Fishman et al., 1986). Such evidence suggests that social organization affects the frequency and manner that rewards are received based on the organizational sophistication of the offenders.

However, this was not present in my findings. There was little evidence that those involved in group-based hacks experienced greater rewards than hackers who offended alone. Most hackers in this study offended on their own and, in some cases, with others. Yet involvement in peer groups and teams did not necessarily translate into frequent involvement in multiple person hacks. The only real evidence of benefits derived from group hacks came from the different competitions at Defcon.

Groups involved in the WiFi Shootout and Scavenger Hunts received public recognition for their skills, as did the teams involved in Root Fu. Nonetheless, the same result occurred for individual competitors like the hacker who won the Wardriving competition. The rewards from hacking did not vary greatly across individuals and groups, indicating hackers did not need to offend with others to benefit from the behavior. Individual hackers could have extended careers in hacking without being affiliated with hacker groups. This challenges the assumptions of social organization research (see Best and Luckenbill, 1994).

Hacker social organization also appeared to have minimal importance in structuring the nature of rewards and benefits of hacking. Instead, the normative orders of hacker subculture influenced the way that individuals derived benefits from hacking. Hackers gained purposive rewards largely focused on mastery of technology, due to its overwhelming importance in hacker subculture. They were able to make computers function in a specific way by hacking either the hardware or software of a system, and could use programs for free after cracking their security programs. Several interviewees also suggested they hacked into university systems to gain free Internet access. However, none of the hackers in any data set reported hacking for monetary gain, which is contrary to many news accounts of hacker activity (see Furnell, 2002).

However, hacking produced expressive rewards that were grounded in hacker subculture and centered on respect and self-improvement. Whether or not a hack was successful, the act of hacking increased the depth of the hacker's connection to technology and improved their understanding of computer operating processes. This carried significant value as an individual's level of knowledge influenced the respect they were shown by others. Hence, performing challenging hacks could be beneficial to one's status in hacker subculture.

There were some reports of emotional benefits from hacking, including feelings of accomplishment and relief. This sense of accomplishment was often derived from hacks that made a computer function properly, or in a new way that it was not designed to do. Completing a challenging hack produced these feelings as well. For instance, Indiana Tones attempted to hack a mail server for some time, but had little success. Once he finally cracked the server, he explained that "it felt, it was nice. It was definitely nice…it helped me keep going." In addition, some hackers reported a sense of fulfillment after hacking to get revenge. Forum users described attacking their school's networks to get revenge against system administrators. Interviewees like Vile Syn hacked out of a need for vengeance. He explained his emotional state after taking down a BBS he was banned from:

> One night I went to [a] friend's house that had a PC and a modem, and quickly logged in to BBS I had been banned from. With my newly acquired hatred for my adversary, I tried a few exploits that I had noticed on other boards. The first and most devastating one I tried was easily used…the feeling of revenge was more than sweet. It was a feeling of accomplishment and overwhelming relief, and remorse was non-existent.

Thus, there were clear emotional benefits derived from hacking that are similar to those experienced in other types of crime (see Katz, 1988). But the norms and values of hacker subculture overwhelmingly influenced the diverse rewards produced from hacking. Considering the benefits of hacking also demonstrates an important relationship between subculture and social organization: subculture plays a role in the development of rewards, while social organization affects the way rewards are received.

Conclusions

This analysis demonstrates the dynamic relationships between subculture, social organization, and behavior. I have found that subculture and social organization structure the nature of deviant relationships, norms, and behavior. At the same time, the nature of deviant acts appears to influence social organization and subculture. While most research examines the effects of subculture or social organization on behavior, my findings indicate that there are greater reciprocal connections between these features of social relationships that must be considered.

For example, the collegial associations between hackers should have limited their ability to complete complex hacks. However, the larger hacker community made resources readily available, allowing individuals to perform difficult hacks. Hacker subculture also placed great emphasis on the need for individual hackers to develop a great deal of skill and ability. Subcultural norms reinforced the importance of sharing information with others, ensuring that hackers need not operate in groups to successfully perform challenging hacks. At the same time, the act of hacking reinforced the social organization practices of hackers by increasing the individual's ability to hack through easy-to-use scripts. The increased ease of hacking has led to the creation of new terms within hacker subculture to negatively label individuals who use such tools.

Furthermore, hacker social organization practices and the nature of hacks may have limited the depth of hacker enculturation. Hackers were introduced to subcultural norms and values through social ties on and off-line, though it was not a complex process. The act of hacking is also geared toward the individual, requiring little immediate assistance from others. This may have affected the normative orders of hacker subculture by articulating the importance of the individual and their need to learn and acquire skills on their own. Hacker identity was constructed and influenced by personal experience and opinions, rather than a group identity. Labels and terms, such as "hacker" and

"blackhat" had multiple meanings within hacker subculture, and may stem from the limited enculturation process of hacker subculture. While the causal relationships between subculture, social organization, and behavior cannot be validated by this study, my findings suggest that fundamental connections exist. This is a significant refinement of our current understanding of the relationships between these constructs and behavior.

The influence of hacker behavior, subculture, and social organization on law enforcement was more apparent. Policing agencies have devised multiple strategies to crack down on hackers, from the creation of task forces to the observation of hacker activities on and off-line. They have also begun to partner with hackers to improve their understanding of hacker methodologies. These relationships allow law enforcement to benefit from subcultural values and norms like knowledge and commitment.

Yet hackers have taken measures to insulate their activities from the threat of sanction. In fact, there were reinforcing relationships present between hacker subculture and social organization on this issue. The hacker community provides informative resources that illustrate how to conceal their activities from police, as well as legal resources in the event of arrest. In turn, hacker subculture provides justifications for behavior and an acute awareness of the threats posed by law enforcement agencies.

Examining the relationships between subculture, social organization, and hacking demonstrated their influence on hacker careers as well. The on and off-line resources made available through the hacker community gave hackers easy access to materials that could keep them continuously involved in deviance without the need for involvement in groups or teams. Hacker subculture affected the internalization of deviant identity through the creation of an argot and labels for behavior based on an individual's knowledge of and commitment to hacking. At the same time,

hackers did not necessarily accept these labels due to the way they constructed hacker identity. Some felt "hacker" was an ideal term that represented a body of knowledge and understanding they could never achieve. The sorts of hacks an individual performed also had some impact on the development of deviant identities. A hacker could choose to engage in hacks that did not violate the law, limiting the creation of a deviant self-identity. As such, the influence of personal opinion and the types of hacks and individual performs may reduce the acceptance of deviant identity, shortening the length of criminal hacker careers.

However, there was no way to verify the actual duration of most criminal hacker careers. The hackers I interviewed had been involved in hacking for some time, though they were not heavily involved in deviant or criminal hacks. Also, these individuals may represent a small proportion of the hacker population. The fact that half of the forums examined for this research no longer operate may be an indication that hackers do not share the same level of commitment (see also Meyer, 1989). In addition, research by Jordan and Taylor (1998) suggests that membership in hacker subculture is dynamic with constant turnover (p.766). Thus, future research would benefit from an examination of the length and nature of criminal hacker careers, to better understand processes associated with desistance from deviant forms of hacking.

Research is also needed to improve our understanding of the benefits derived from hacking. My analysis suggests that social organization structures the way that individuals receive rewards from hacking. Hackers appeared to obtain the same benefits from hacking regardless of whether they operated alone or in groups. These rewards were shaped by the normative orders of hacker subculture, including the ability to improve their computers and software through purposive hacks. Hackers derived expressive benefits from hacking, including an increased level of knowledge, deeper connection to technology, and greater respect and status. On the other hand, there was little

to no evidence of monetary or illicit gains from hacking. Although hackers did use cracked software and occasionally stole Internet access, there were no hacks reported where the perpetrator obtained monetary rewards in any of the data sets.

This contradicts many of the media reports emphasizing the economic impacts and benefits of hacking (see Furnell, 2002). This issue requires further examination with a sample of known criminal hackers who have benefited economically from hacking. Such a population may demonstrate the importance of economic and non-monetary benefits for hacker activity. Furthermore, this could expand our understanding of the importance of achievement on continued engagement in criminal behavior (see Morselli and Tremblay, 2004).

As a whole, this analysis has demonstrated the value of exploring the connections between subculture, social organization, and deviant behavior. Each factor shapes the other, though these influences are not readily apparent when only considering the affects of subculture or social organization on behavior. However, I cannot validate the causal relationships that I have identified and they may not be applicable across all crime types. Research is needed using different populations of offenders to identify and explore the influences between these sociological constructs and criminal behavior. This can refine our understanding of the relationships between subcultural norms, interpersonal relationships, and behavior across criminal and deviant groups.

SUMMARY

This dissertation examined the social organization and subculture of computer hackers, as well as the relationships between these two sociological concepts and behavior using multiple qualitative data sets. These are critical issues in criminology as they address the nature of criminal behavior, associations, and organization. Exploring the social nature of computer hacking is necessary to better understand this increasingly prominent, yet misunderstood crime type (see

Furnell, 2002). Research from the social sciences (see Wall, 2001; Schell et al., 2002) and computer sciences (see Furnell, 2002; The Honeynet Project, 2001) has improved our knowledge of computer crimes. Still, there are several issues that require clarification, especially regarding computer hackers. I identified three of these research avenues in Chapter One.

Specifically, a number of studies on hacker subculture have identified the values, norms, and beliefs of hackers and demonstrated the influence of subcultural involvement on hacker behavior (Meyer, 1989; Jordan and Taylor, 1998; Taylor, 1999; Loper, 2000; Thomas, 2002; Wysocki, 2003). However, constant shifts in technology may affect the elements that compose this subculture over time. These depictions of subculture may also vary due to the sampling and methods used (see Short, 1968). As such, one goal of this dissertation was to examine hacker subculture to expand our knowledge of its value systems and impact on hackers.

Furthermore, research on the social organization of computer hackers has the potential to increase our knowledge of how these individuals operate within the subculture individually and in group contexts (Best and Luckenbill, 1994). Yet the only study to examine this issue was performed over 15 years ago (Meyer, 1989). Utilizing the Best and Luckenbill (1994) framework of organizational sophistication, Meyer found that hackers were colleagues and in some cases peers, but their offenses and culture did not promote any further organizational sophistication. At the same time, evidence presented by researchers (Denning, 2001) and the media (MENA Business Reports, 2002) indicates that hackers may be operating in more formal organizations due to changes in computer technology and its use. Thus a second goal of this dissertation was to examine the social organization of computer hackers.

Finally, I considered an important research issue regarding concepts within sociology and criminology. Very few researchers have considered how the subculture of a criminal group

influences its social organization and vice versa. The way that deviant acts structure subcultural norms and social organization has also not been explored in detail. Instead, most research only considers the relationship between subculture or social organization and behavior, and tends to assume a unidirectional affect. As a result, our knowledge of the relationships between these sociological constructs and behavior is limited. Hence, I sought to explore the relationships between the organizational practices of hackers, normative orders of hacker subculture, and the act of hacking using the findings from my analyses.

Chapter Two outlined the nature of the various data sets I developed to perform this research, which included 365 strings from hacker web forums, interviews with active hackers, and observations made at the Defcon hacker convention. Using multiple data sources provided a way to examine hackers in cyberspace and meatspace. I also triangulated the data to consider any patterns of evidence across the data sets, while addressing how the social setting and context of each data source could affect the findings. This methodology enabled me to generate rich and diverse insights on the behaviors and relationships of hackers on and off-line. Future research should continue to use multiple data sources and triangulation, as this is a productive way to access this hidden population of offenders (see also Meyer, 1989; Loper, 2000; Wysocki, 2003).

In Chapter Three, I explored hacker subculture using the concept of normative orders, which are a "set of generalized rules and common practices oriented around a common value" that structure and justify behavior (Herbert, 1998: 347). Normative orders provide a dynamic view of culture, recognizing the influence of both individual decision-making and subcultural values on behavior. This perspective was especially useful when combined with grounded theory techniques, demonstrating its value for researchers interested in examining the ways individual behavior is structured in the context of subcultures.

I found that the social world of hackers was shaped by five normative orders: technology, knowledge, commitment, categorization, and law. These orders were interrelated, and overwhelmingly influenced by technology. In fact, the connection between hackers and technology was possibly the most important order of hacker subculture because it structured the interests and activities of hackers on and off-line (see also Jordan and Taylor, 1998; Taylor, 1999; Thomas, 2002). For example, hackers focused a significant amount of time and effort into learning and understanding the various facets of computer technology. As a result, technology was intimately tied to knowledge and commitment.

Knowledge was also used to justify hacking, as some hackers suggested they pushed technology to its limits to understand the boundaries and potential of computers. The exchange of information with potential illegal applications could be rationalized as a way to educate others. Hackers based subcultural status and labels on an individual's comprehension of and connection to technology. Individuals with demonstrable skill and ability were shown a great deal of respect and were referred to as hackers. However, poorly skilled hackers with no interest in developing their skills were called script kiddies and shown very little respect. These labels indicated the importance of commitment to hacking in structuring how others viewed and defined their actions within subculture.

However, the order categorizations recognized the influence of individual opinion in constructing hacker identity. Hackers discussed the meaning of labels, like white and black hat hackers, and the various activities of these individuals. There was some variation in the meaning of these terms across hackers, demonstrating that a hacker's beliefs about whom and what constituted a hacker and hack were dependent upon personal opinion.

Finally, the order law detailed the way that hackers identify and relate to the law. Hackers spent some time discussing the legal nature of hacks and whether or not they should be performed. Many hackers suggested the act of hacking should not be illegal because it produced beneficial results for the larger population of computer users. Thus, hackers used this belief to justify their activities. Also, hackers created boundaries between themselves and law enforcement, though these boundaries were somewhat permeable due to increasing cooperation between the two groups.

These normative orders structure hacker subculture in much the same way as other criminal groups that develop subcultures, including skinheads (Hamm, 1993), professional thieves (McIntosh, 1975), drug dealers (Adler, 1993), and youth gangs (see Miller et al, 2001). These subcultures all offer norms, values, and beliefs that influence individual behavior and help to form deviant identities. They also create boundaries and codes of conduct that structure how the group relates to the larger culture. A unique argot is present in each subculture, as well as ways specific behaviors or actions generate status and respect for members. This suggests that hackers do share common ground with other types of criminals, despite arguments over the ways criminologists should consider the activities of computer criminals (see Wall, 1999; Barlow, 1992).[29]

In Chapter Four, I investigated the social organization of hackers using concepts derived from Best and Luckenbill's (1994) continuum of organizational sophistication. I also incorporated elements from research by Decker et al. (1998) on the complexity of divisions of labor, coordination of roles, and purposiveness of associations between hackers to assess their current state of social organization. My findings indicated that hackers were not loners, but rather colleagues who had relationships with other hackers in meatspace and cyberspace (see also Meyer, 1989). These

---

[29] Computer crime researchers have argued over whether crimes committed in cyberspace are "old wine in new bottles", or if the unique characteristics of these crimes coupled with the new realm of cyberspace constitutes "new wine in new bottles" (Wall, 1998:202; Wall, 1999; Barlow, 1992).

connections were used to share information and introduce subcultural norms to new hackers although hacking was largely a solitary activity. Furthermore, hackers formed peer groups, which had little stratification or role specialization (see also Meyer, 1989). These groups facilitated the exchange of information and resources between members, and occasionally performed group-based hacks. In addition, a limited number of teams were present in the data with specialized roles and divisions of labor when hacking, though this was largely reserved for the unique setting provided by the Defcon convention.

I also found that there has been some change in hacker social organization since Meyer's (1989) study was completed. For instance, there now appear to be legitimate formal hacker organizations within hacker subculture, such as the Defcon convention. The convention had all the characteristics of organizational sophistication, yet the convention organizers did not promote deviant or criminal behavior. Moreover, I found that hackers now constitute a community, on the basis of common territories and institutional completeness. Hackers have shared spaces in cyberspace through various forms of computer mediated communication, and in meatspace via hacker conventions. The community appears to be institutionally complete due to the multitude of institutions providing goods and services for hackers.

The social organization practices of hackers share some similarities with other criminal groups. Specifically, the loosely organized peer groups formed by hackers are comparable to those of disorganized youth gangs (see Decker and van Winkel, 1996). Neither hacker peer groups nor neighborhood based gangs have clearly defined roles, leadership structures, or formal rules for members. Furthermore, the loose overlapping networks that compose the hacker community mirror the organizational practices of fences (Steffensmeier, 1986) and drug smugglers and dealers (Adler

and Adler, 1983). As with hackers, each of these groups use their social ties to gain access to myriad resources including supplies to engage in crime and develop social connections with other deviants.

However, not all facets of hacker organization fit within Best and Luckenbill's (1994) ideal types. The categorization of web forums is complicated by their two-population composition: forum users and forum operators or moderators. Individuals with loose connections to one another that did not necessarily offend together composed the broader user group, while the smaller group of forum moderators could be considered a team based on their clear division of labor, stratification, and rules on the behavior of members. Thus, the forums did not clearly fit within the continuum of organizational sophistication, though the authors recognize that their framework consists of ideal typologies (Best and Luckenbill, 1994: 13). As a result, it is possible that groups may fall between or outside of their classification scheme.

This research suggests that further refinement and conceptual development is needed to explore the contours of Best and Luckenbill's (1994) continuum of organizational sophistication. Their frame allowed me to differentiate between forms of organization based on the peer relationships of hackers, and assess their impact of these organizations on hackers' ability to offend. However, Best and Luckenbill (1994) did not fully operationalize the concepts that structure their framework. The inclusion of measures from Decker et al.'s (1998) research helped overcome this limitation by addressing the ways that individuals relate to one another, the division of labor in groups, and any between-group interactions. Hence, continued integration of conceptual elements from each of these studies could prove invaluable to future research on deviant social organization.

In this final chapter, I considered the interrelated nature of hacker subculture, social organization, and hacker behavior. Though researchers have frequently used these concepts individually to examine criminal behavior, the connections and relationships between these

constructs have rarely been explored. Researchers have also infrequently considered how deviant acts may shape subculture and social organization, particularly when innovations change the nature of the behavior. Examining these issues in tandem allowed me to consider how social organization, subculture, and deviant behavior affect the nature and structure of each.

There were clear connections between hacker subculture, social organization, and hacking, especially concerning the ability to complete complex hacks. These findings demonstrated the significant influence of access to resources for both social organization and deviant behavior. In addition, there were instances in which one had more influence over the other, as with hacker enculturation. The organizational sophistication of hackers and individual orientation of hacks appear to weaken the enculturation process of hackers. In turn, the normative orders of hacker subculture emphasize the individual and allow for interpretation of hacker identity. Also, the normative orders of hacker subculture and the act of hacking structured the development of hacker identity and rewards from hacking. At the same time, hacker social organization affected the way that individuals received benefits from hacking and facilitated hacking by providing access to necessary resources.

This analysis demonstrated the significance of examining subculture, social organization, and deviant behavior in tandem. The results provide both support for and challenges to assumptions about the relationships between subculture, social organization, and behavior. However, the strength of these conclusions are tenuous and may only apply to computer hackers. As such, further exploration of the relationships between these sociological constructs and behavior is needed to expand of the interconnections and influences present. Such research could improve our knowledge of the extent to which the nature of the deviant act itself actually shapes social organization and subculture.

Policy Implications

The results of this research provide limited guidance for policy makers. Hackers in this research did not report involvement in malicious hacks against important financial or government targets. Rather, they hacked to understand how computers operate, obtain free software or Internet access, and gain status within hacker subculture. Thus, this study presented an image of hackers engaging in relatively limited forms of deviance. This is not to suggest that the activities of computer hackers should be ignored; the knowledge and skill of most hackers could pose a threat to the safety of personal information and data stored on-line. However, it is difficult to provide strong policy recommendations for law enforcement based on the limited criminal behavior of these hackers.

Still, there is one policy implication that can be drawn from my findings. This study clearly demonstrated that hackers take an early interest in technology. Many of the interviewees described developing an interest in computers and technology in their youth. In turn, this may explain why many forum users and some interviewees described hacking their school's computer networks. Identifying technically savvy youngsters in schools and at home and channeling their activities into productive legitimate avenues may be a way to reduce the criminal behavior of hackers. Providing outlets at school, such as assisting system administrators, can give young hackers ways to learn and apply their skills in a productive fashion. Such positions could prime them for later work in the IT field.

A limited number of programs providing outlets for technologically oriented youth exist, such as the Utah CyberCorps program.[30] This provides middle and high school students with

---

[30] None of the programs currently operating explicitly state that they are trying to divert computer hackers away from criminal behavior. However, they do provide excellent opportunities for skilled hackers to utilize their talents in a productive, legal manner.

training in areas like network troubleshooting and pc repair (CyberCorps Boot Up Camp August 8-9, 2005). After completing their training, the students are placed into technology support positions within their school to assist students and staff. There is also a federally sponsored Cyber Corps program that provides college scholarships to students interested in technology (Office of Personnel Management, 2004). The goal of this program is "to increase and strengthen the cadre of federal information assurance professionals that protect the government's critical information infrastructure" (Office of Personnel Management, 2004). Thus, students who receive these scholarships are expected to work for a federal agency for a period of time after they graduate. While the efficacy of these programs has not yet been evaluated, they may prove useful in guiding interested young people into legitimate applications of their knowledge and skill.

Implications For Future Research

The results of this study also have multiple implications for future research, as there are several issues that require further exploration to expand our understanding of hackers. To begin, this dissertation highlights the need for research exploring the nature of hacker careers. My findings suggest that the hacker community may facilitate long term involvement in hacking, while the act of hacking and hacker subculture had contradictory influences. The individual nature of hacker identity coupled with involvement in legal hacks may limit the acceptance of deviant labels, and effectively reduce the duration of criminal hacker careers. However, there is no clear evidence on the duration of hacker careers or what issues affect desistance from hacking. Jordan and Taylor (1998) suggest that membership in hacker subculture is dynamic with constant turnover, although this finding has not been refuted or supported by other research. Thus, there is a need to explore the onset, duration, and desistance of hackers. Such information can shed some light on the nature of hacker careers and assess any similarities between hacker careers and those of the larger offender population.

In addition, it would be beneficial for researchers to further examine the structure of hacker organizations. While I found some sophisticated hacker organizations, there was limited detail on their leadership, rules, and operations. This was due in part to the small number of interviewees who belonged to hacker groups, and was compounded by my limited access to many of the groups at Defcon. Identifying and interviewing hackers who have belonged to groups could refine our understanding of the nature of these groups, and the benefits provided by membership. Moreover, this may clarify the importance of groups and formal organizations within this relatively collegial hacker subculture.

Such research may help clarify the significance of formal groups like the Tamil Tigers and Zapatista rebels who engage in hack-based cyber-attacks. There was no real evidence of individuals who belong to these sorts of groups within this data, though there is growing research that hacktivists, cyberterrorists, and cyber-protestors are utilizing hackers (see Jordan and Taylor, 2004). Research focusing on the nature of such hacker groups may shed light on the way these individuals are viewed by other hackers. This may provide insight on the use of hacking as a means to an end, rather than as an activity with its own intrinsic value, as was the case in the current study.

Another important implication of this dissertation is the need for research on the existence of multiple hacker subcultures. Many of the hackers discussed the way that black hats, script kiddies, and crackers differed from other types of hackers. Some interviewees implied that the experiences and activities of criminal hackers were somehow different from their own. Gaining access to a more diverse cross section of the hacker population may provide some insight into the way different types of hackers experience hacker subculture. This may highlight any schisms between criminal and non-criminal hackers and inform our knowledge of the importance of monetary and non-economic

rewards for hackers. Examining the experiences of manifold types of hackers could expand our understanding of hacker subculture and hacking generally.

It would also be helpful to consider why there are so few women involved in hacking. It was clear from this research that hacking is a relatively male dominated activity (see also Jordan and Taylor, 1998). As noted in Chapter Two, none of the interviewees and very few of the forum users were known females. Women comprised a small percentage of the Defcon population. Reasons for this gender gap have not been well explored (but see Jordan and Taylor, 1998), and most who have studied this issue have used largely anecdotal rather than empirical evidence (see Gilboa, 1996; Keller, 1988). As such, it is necessary to examine the gendered experiences of hackers to consider why this disparity exists, how male dominated organizational structure affects hacker subculture, as well as any differences in the activities of male and female hackers (see also Turkle, 1984). Such research could also demonstrate any links between the experiences of female hackers and those of the larger population of female offenders.

This dissertation has explored concepts that are often studied separately by sociologists and criminologists. By concurrently examining hacker subculture, social organization, and behavior, I have found dynamic relationships that affect the nature and structure of each. Most researchers assume that subculture or social organization influence behavior, but do not consider the presence of any reciprocal relationships. My research provides compelling evidence that criminologists and sociologists should explore the links between these sociological constructs and behavior with different criminal groups. This could refine our knowledge of the relationships between and manner in which subculture, social organization, and the nature of deviant acts affect one another.

A final implication of this study is the need for cross-disciplinary research on computer hackers. There has been little collaboration between researchers in the social and computer sciences.

Bringing researchers from these two fields together could greatly increase the quality of research because each field could inform the other. Computer scientists could provide insight into the technical aspects of hacks and other computer crimes, and social scientists could highlight what social and individual factors may drive these behaviors. This would ensure a more comprehensive understanding of computer crimes, rather than piecemeal investigations that do not take advantage of the strengths of each discipline. Such research may prove vital for technicians and law enforcement to deal with this increasingly important, yet misunderstood crime type.

GLOSSARY OF KEY TERMS

BASIC: acronym for Beginners All-purpose Symbolic Instructional Code. An easy-to-learn, highly flexible computer language invented at Dartmouth University. Different versions of BASIC run on various operating systems. Since each version has its own peculiar quirks, a BASIC program written in one version may not be compatible with another version.

www.netdictionary.com/b.html

Binary: 1. code and binary files are information and commands stored and used by hardware and software in their most elemental form--strings of on-off signals to an electronic processor. Many systems of binary encoding of data and commands are proprietary and unique to particular hardware and software systems. They are usually the most compact means of storing data, and commands stored in binary form can execute very rapidly, but binary files often are difficult to transfer between differing computer systems. Often binary files are translated into ASCII form for transfer between computers. www.colorado.edu/geography/gcraft/gloss/glossary.html 2. numbering system based on two digits: 0 and 1. www.crucial.com/library/glossary.asp

Black Hat Hacker: a skilled hacker who breaks into systems without authorization or permission to engage in malicious behaviors, such as damaging or corrupting data (also blackhat hacker, black-hat hacker).

Bulletin Board System (BBS): a computerized meeting system created by direct modem-to-modem connections over a phone line, using a single computer as a server. BBS users can have discussions, make announcements, and upload or download files. The BBS is the forerunner of the web forum.

Common Gateway Interface (CGI): A set of rules that describe how a Web Server communicates with another piece of software on the same machine, and how the other piece of software (the "CGI program") talks to the web server. Any piece of software can be a CGI program if it handles input

and output according to the CGI standard. Usually a CGI program is a small program that takes data from a web server and does something with it, like putting the content of a form into an e-mail message, or turning the data into a database query.

free-web-site-hosting.biz/web-hosting-glossary.html

Cracker: 1. a hacker who engages in malicious or damaging hacks. 2. someone who breaks the security and protections on software enabling them to use or copy the materials at any time for free.

Cryptograhpy: the art of science concerning the principles, means, and methods for rendering plain text unintelligible and for converting encrypted messages into intelligible form.

www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html

Cyberterrorist: terrorist who uses hacks and technology-based attacks to threaten or attack systems, networks, or data to coerce or intimidate another party under the guise of a political or social agenda.

Dameware: an enterprise system management application for Windows NT/2000/XP. It provides an integrated collection of Windows NT/2000/XP administration utilities incorporating a centralized interface for remote management of Windows NT/2000/XP Server and Windows NT/2000/XP Workstation machines.

Disk Operating System: the original operating system for PC-type computers that provides instruction to enable computer to interpret keyboard and mouse input, display information on the screen, control printer, and work with other hardware attached to the computer.

www.park-meadow.org/computer_terms.htm

Denial of Service Attack (DoS): attack which prevents legitimate access to systems or services due to activities originating from unauthorized system users.

Elite: a very skilled, proficient hacker (also 'leet, leet, 1337).

Exploit: a hole, flaw, or vulnerability in a computer program or network that can be used to attack and enter a system.

File Transfer Protocol: a standard that allows users to transfer files from one computer to another using a modem and telephone lines. www.wda.org/Public/help/glossary.htm

Firewall: a security system enforcing the boundary between two or more networks which permits or denies the transfer of data based on security policies.

Hacker: 1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. 2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming. 3. A person capable of appreciating hack value. 4. A person who is good at programming quickly. 5. An expert at a particular program, or one who frequently does work using it or on it; as in `a Unix hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate.) 6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example. 7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations. 8. [deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence `password hacker', `network hacker'. The correct term for this sense is cracker. http://www.science.uva.nl/~mes/jargon/h/hacker.html

Hacktivist: hackers who break into computers to further an activitist agenda.

Information and Communications Technology (ICT): Information Technology (IT) or Information and Communication Technology (ICT) is the technology required for information processing. In particular the use of electronic computers and computer software to convert, store, protect, process, transmit, and retrieve information from anywhere, anytime.

en.wikipedia.org/wiki/Information_and_Communications_Technology

Instant Message (IM): like a chat room, IM is used to send messages back and forth through the Internet to a specific user. It is like a chat room in the way that you can communicate, but unlinke a chat room unless in a private chat the information that is being typed is sent directly to the user and is not viewed by anyone else.   web.uncg.edu/dcl/icampus/access/glossary.asp

Internet Protocol (IP): Internet Protocol specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher- level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source. IP by itself is something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.   www.channelstorm.com/Manual/Data/GL00/GL00.htm

Internet Service Provider (ISP): an Internet Service Provider provides access to the Internet for others via some connectivity service(s). This might be in the form of dial up services, web hosting services or the combination of both.   domain.rshweb.com/glossary.html

Intrusion Detection System (IDS): an automated system that can detect a security violation on a system or a network. docs.hp.com/en/J5083-90011/ch01s06.html

Lol: abbreviation for "laughing out loud"

Lamer: a negative term ascribed to hackers who engage in either criminal or negative behaviors. Also applied to hackers engaging in relatively weak hacks.

mIRC: a shareware Internet Relay Chat client for Windows, created in 1995 and developed by Khaled Mardam-Bey. This was originally its only use, but it has evolved into a highly configurable tool that can be used for many purposes due to its integrated scripting language.

en.wikipedia.org/wiki/MIRC

Malware: a collective term for a variety of malicious software programs, including viruses, worms, and Trojan Horses.

Newbie: someone who is either new to hacking or web forums (also noob, n00b, newb).

Password Cracker: a program used to break passwords in any sort of system, program, or network.

Peer To Peer: a type of Internet network that allows users with the same program to connect with each other and access files on one another's hard drives. (also P2P p2p)

www.techliving.com/article/353.html

Penetration Testing: security testing where an individual attempts to circumvent the security features of a system. This is an activity that legitimate security professionals and white hackers frequently engage in to assess the weaknesses of systems (also pentest).

Poledit: the System Policy Editor for Microsoft software which is a powerful security tool to help limit user access.   http://www.zisman.ca/poledit/

Phreaker: individual who hacks telephone networks and related technologies.

Port Scanner: a program that probes specific systems and identifies the Internet services it is running. This tool is often used to identify targets based on known vulnerabilities within the services used by that computer.

Proof of Concept Code: programming code that demonstrates or identifies an exploit within a system that can be attacked (also POC).

Random Access Memory (RAM): a type of computer storage whose contents can be accessed in any order. This is in contrast to sequential memory devices such as magnetic tapes, discs and drums, in which the mechanical movement of the storage medium forces the computer to access data in a fixed order. en.wikipedia.org/wiki/RAM

Regedit: registry editor supplied by the Windows NT operating system for manually editing the NT

Registry.   www.starquest.com/Supportdocs/starsqldocs/StarSQL/Glossary.htm

Registry: in Windows 2000, Windows NT, Windows 98, and Windows 95, a database of

information about a computer's configuration. The registry is organized in a hierarchical structure

and consists of subtrees and their keys, hives, and entries.

www.pegusisfreeware.com/htmltools/Resource_Info/resource_info_7.htm

Remote Administration Tool: a program that allows a user to remotely monitor and control a

targeted system. These programs are sent to the target often through trojan horse programs that,

once opened, allow the user to gain control over the system. Sub7 is one example of such a

program.

Rootkit: a hacker tool that provides a backdoor into a system and conceals the penetration point and

any indications that the system has been compromised.

Scene Whore: individual who is not involved in hacking or hacker subculture but attends hacker

conventions and fraternizes with hackers.

Script Kiddie: hacker with very limited skill who relies on scripts or programs created by others to

perform actual attacks. More skilled hackers view script kiddies as the cause of a great deal of

malicious attacks.

Secure Sockets Layer (SSL): a protocol developed by Netscape for transmitting private documents

via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL

connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use

the protocol to safely transmit confidential information, such as credit card numbers.

www.techniqueweb.com/terminology.php

Structured Query Language (SQL): an industry-standard language for creating, updating and, querying relational database management systems.

www.ru.ac.za/library/theses/2003/halse/ft/html/glossary.html

Sub7: a well known Remote Administration tool whose use is often attributed to script kiddies.

Virus: a replicating program that enters a system concealed in infected files, disks, or documents. Once the infection occurs, the virus delivers a payload that has damaging or unexpected side affects.

W32Dasm: a disassembler and debugger for 16/32 bit windows applications, by URSoft.

www.expage.com/page/w32dasm/

Wardriving: driving around a city or area using a laptop and various pieces of equipment to look for unsecured wireless Internet (or wi-fi) access points.

Warez: cracked or pirated software often traded between hackers.

Web Forum: an online center for ongoing, in-depth discussions of specific topics and issues organized into discrete categories (also called a bulletin board or message board).

Web Forum Post: the basic building block of web forums. Individuals provide their opinions or pose questions in a post to the forum.

Web Forum String: a series of posts along a specific topic or issue. Each string begins with a post containing a comment or question drawing feedback from others who post to this message. Thus, strings are composed of posts linked together.

White Hat Hacker: a skilled hacker who uses their knowledge and skill to protect and secure systems (also whitehat hacker, white-hat hacker).

Wi-Fi: abbreviation for "Wireless Fidelity". This is a set of standards for wireless local area networks developed for use by wireless devices and local area networks. It is now commonly used for Internet access when an individual is in range of an access point or hotspot.

APPENDIX A

Face to Face Interview Guide

   Thank you again for your willingness to be interviewed and I want to again assure you that we can stop this interview any time you want. I am going to ask you some questions and would like this to be more of a conversation than an "interview" or something very formal.
   Everything you say will be kept confidential and no one will know what we've talked about. After this is over, I will not have a record of your real name, only the name you want to be identified by, so your actual identity will be kept secret. This will also ensure that no one will be able to link this interview to you personally.
   Now the law may require me to report to the authorities any statements you might make about planning to deface or hack any specific sites or targets in the future. I will not be asking you questions about that sort of thing, and I do not want you to tell me about anything that fits this description either, so we will both be safe.
   Also, you do not have to answer any questions you feel are inappropriate, talk about anything you feel uncomfortable discussing, and you can end this interview at any time. I would prefer to record our interview so that I will remember the information that you provide as accurately as possible. Once I transcribe the tape, I will erase it so it cannot be later identified to you. Is it o.k. to turn on the recorder? Then let's begin.

1. When and how did you develop an interest in computers and technology?
   Who or what kept your interest?
   What did you do to get further involved in computing?
   How did you learn what to do?

2. When and how did you develop an interest in hacking?
   Who or what kept your interest?
   What did you do to get further involved in hacking?
   How did you learn what to do?

3. Can you tell me about the first time that you ever performed a computer hack?
   What did you do?
   What was the target?
   How did you know what to do?
   How did it make you feel?
   Did you want to do it again and why?
   Were others present with you at the time, either on-line or physically with you?
   How old were you?
   Were you using your computer or someone else's equipment?

4. How soon after this hack did you perform another hack?
   What made you want to do it again?

5. How do you identify targets?

6. How would you characterize the majority of your hacks? (i.e. purposeful, malicious,)

7.   Do you only perform a specific task within a hack, or can you do a variety of things?

8. What would you say was your most successful hack?
> What made it successful?
> What did you do?
> Did you need help to do it?

9. What was the most difficult hack you have performed?
> What made it difficult?
> What did you do?
> Did you need help to do it?

10. If you needed or wanted to perform a hack but did not have all of the equipment or knowledge to do it, how would you get the materials or information to do it?

11. What are some of the other ways that hackers can get information on targets, systems, and hardware?

12. Have you ever visited a web forum or BBS for hackers? If yes, how would you describe the experience?
> Did you go there often?
> Did you make any friends through the forum or BBS?
> Did you get information or knowledge on hacking from the posts?
> Do you feel the experience improved your skill as a hacker?

13. Do you consider yourself a hacker? If yes, how did you know you were one?

14. How do you define a hacker?

15. What does it mean to be a hacker?

16. Do you think it is wrong to either maliciously break into or knowingly damage a system? Why or why not?

17. Is there a hacker community or culture? If yes, how would you define it?

18. If a hacker community or culture exists, what are the most important elements of it?

19. Do you have any friends or associates who are hackers?
> How did you meet them?
> How many of your friends are hackers?
> Why do they hack?
> Have you ever helped them perform a hack? If so when and how?
> What other activities do you do with these friends aside from hacking?

20. How frequently do you perform hacks alone? With others?
    If you have hacked with others, are they more involved or complicated than hacks
    attempted by you alone?

21. Are there any outward physical signs that suggest an individual is involved in hacking?

22. What would make you stop hacking?
    What would make any of your friends who hack stop hacking?

23. Do you think hacking should be illegal? Why or why not?

24. Can you think of any ways to stop hackers from doing what they do?

25. Please tell me what you think the following terms mean, and how likely you are to use them
    when talking to other hackers?
    Black Hat

    White Hat

    Script Kiddie

    Hacker Gang

    Hacktivist

    Cyber Terrorist

    Cracker

26. Are there any terms not listed here which you feel are important or often use to describe a
    hacker? Why are they important to you?

27. Is there anything that I have not asked about that you think I should know, or anything you
    want to talk about?

28. Can you provide any contacts with other hackers that may be willing to engage in an
    interview?

    That is all that I have to ask, so we can stop the tape. I appreciate your time and all of the
    information you have provided. If there are any problems or any further questions regarding the
    information you have provided, may I contact you again? Thank you and I appreciate your time.

.

APPENDIX B

<u>E-mail Interview Questionnaire</u>

Please answer the following questions as truthfully and fully as you can. Use the questions underneath each numbered question as a guide for your answer. You can skip any question you do not want to answer and may stop the interview at any point you wish. Please understand that your answers will be used for academic research ONLY, and any information you provide will be strictly confidential and your privacy protected. The more quickly you return this questionnaire, the greater the likelihood that your answers will be included in the final written paper and receive the $10 money order compensation for completing the form.
To ensure your protection, please DO NOT provide any information on any illegal activities you plan on performing in the future (for example, DO NOT say that you are planning to hack into a government website next week), and use a name that you would like to be referred to for the purposes of this research that is not in any way, shape, or form your REAL name.

Please provide the name you would like to be referred to here: _____

1. When and how did you develop an interest in computers and technology?
    Who or what kept your interest?
    What did you do to get further involved in computing?
    How did you learn what to do?

2. Can you tell me about the first time that you ever performed a computer hack?
    What did you do?
    What was the target?
    How did you know what to do?
    How did it make you feel?
    Did you want to do it again and why?
    Were others present with you at the time, either on-line or physically with you?
    How old were you?
    Were you using your computer or someone else's equipment?

3. How soon after this hack did you perform another hack?
    What made you want to do it again?

4. How do you identify targets?

5. How would you characterize the majority of your hacks? (i.e. purposeful, malicious,)

6. Do you only perform a specific task within a hack, or can you do a variety of things?

7. What would you say was your most successful hack?
    What made it successful?
    What did you do?
    Did you need help to do it?

8. What was the most difficult hack you have performed?
       What made it difficult?
       What did you do?
       Did you need help to do it?

9. If you needed or wanted to perform a hack but did not have all of the equipment or knowledge to do it, how would you get the materials or information to do it?

10. Do you consider yourself a hacker? If yes, how did you know you were one?

11. How do you define a hacker?

12. What does it mean to be a hacker?

13. Do you think it is wrong to either maliciously break into or knowingly damage a system? Why or why not?

14. Is there a hacker community or culture? If yes, how would you define it?

15. If a hacker community or culture exists, what are the most important elements of it?

16. Do you have any friends or associates who are hackers?
       How did you meet them?
       How many of your friends are hackers?
       Why do they hack?
       Have you ever helped them perform a hack? If so when and how?
       What other activities do you do with these friends aside from hacking?

17. How frequently do you perform hacks alone? With others?
       If you have hacked with others, are they more involved or complicated than hacks
       attempted by you alone?

18. What would make you stop hacking?
       What would make any of your friends who hack stop hacking?

19. Do you think hacking should be illegal? Why or why not?

20. Can you think of any ways to stop hackers from doing what they do?

21. Please tell me what you think the following terms mean, and how likely you are to use them when talking to other hackers?
       Black Hat

       White Hat

       Script Kiddie

Hacker Gang

Hacktivist

Cyber Terrorist

Cracker

Thank you again for completing this questionnaire and if you have any questions regarding the questions posed, please contact me via e-mail at diydissertation@yahoo.com or by phone at 314-516-4914.

When you have completed the form, please send it back to me and provide an address where your money order can be sent. Please remember that all of the information you have provided will be kept confidential and anonymous, and you will be referred to in any publications by the surname you have provided.

Thomas Holt
Graduate Student/Adjunct Lecturer
Department of Criminology and Criminal Justice
University of Missouri-Saint Louis
543 Lucas Hall
8001 Natural Bridge Road
Saint Louis, MO, 63121

REFERENCES

2600 Meeting Guidelines. [Online] Available http://www.2600.com/meetings/guidelines.html,

      Accessed September 4, 2003.

Abadinski, H. 1990. *Organized Crime,* 3rd ed. Chicago, IL: Nelson-Hall.

Adler, P.A. 1993. *Wheeling and Dealing: An Ethnography of an Upper-Level Drug Dealing and*

      Smuggling Community, 2nd ed. New York: Columbia University Press.

Adler, P.A., and Adler, P. 1983. Shifts and Oscillations in Deviant Careers: The Case of Upper-

      Level Drug Dealers and Smugglers. *Social Problems* 31: 195-207.

Agnew, R. 1995. Strain and Subcultural Theories of Criminality. Pp. 305-327 in Sheley, J.F. (Ed.)

      Criminology: A Contemporary Handbook. Belmont, CA: Wadsworth Publishing.

Anderson, E. 1999. *Code of the Street.* Philadephia, PA: W. W. Norton.

Barlow, J.P. 1990. *Crime and Puzzlement.* [Online] Available

      http://www.eff.org/Publications/John_Perry_Barlow/crime_and_puzzlement.1, Accessed

      January 29, 2004.

_____. 1992. *Selling wine without bottles; the economy of mind on the global net.* [Online]

      Available http://selenasol.com/selena/extropia/idea_economy_article.html, Accessed January

      29, 2004.

Best, J. and Luckenbill, D.F. 1994. *Organizing Deviance, 2nd edition*. New Jersey: Prentice Hall.

Black Hat USA FAQ 2005. [Online] Available http://www.blackhat.com/html/bh-media-

      archives/bh-archives-2004.html, Accessed March 15, 2005.

Blumer, H. 1969. *Symbolic interactionism.* Englewood Cliffs, NJ: Prentice Hall.

Brake, M. 1980. *The sociology of youth cultures and youth subcultures.* London: Routledge and

      Kegan Paul.

Chambliss, W. J. 1972. *Box Man.* New York: Harper and Row.

Cheung, H. 2004. *Defcon 12's Fear and Hacking in Vegas.* [Online] Available

   http://www4.tomshardware.com/business/200408021/index.html, Accessed, April 15, 2005.

Clinard, M.B. and Quinney, R. 1973. *Criminal Behavior Systems, 2nd Edition.* New York: Holt,

   Rinehart, and Winston.

Cohen, A. K. 1955. *Delinquent Boys: The culture of the gang.* Glencoe, IL: Free Press.

Computer Security Institute. 1998. *An e-mail attack on Sri Lanka computers*. Computer Security

   Alert No. 193, June, p.8.

Corbin, J. and Strauss, A. 1990. Grounded Theory Research: Procedures, Canons, and Evaluative

   Criteria. *Qualitative Sociology* 13(1): 3-21.

Cressy, D.R. 1969. *Theft of the Nation.* New York: Harper and Row.

_____. 1972. *Criminal Organization.* New York: Harper & Row.

CyberCorps Boot Up Camp August 8-9, 2005. [Online] Available

   http://www.cybercorps.k12.ut.us/bootup.html, Accessed May 29, 2005.

Decker, S. H. and Van Winkle, B. 1996. *Life in the gang: Family, friends, and violence*. New

   York: Cambridge University Press.

Decker, S. H., Bynum, T., and Weisel, D. 1998. A Tale of Two Cities: Gangs as Organized Crime

   Groups. Pp. 73-93 in Miller, J., Maxson, C. L., and Klein, M. W. (Eds.) *The modern gang*

   reader. Los Angeles, CA: Roxbury Publishing Company.

Defcon. 2005a. *Past Defcons*. [Online] Available http://www.defcon.org/html/links/past-

   defcons.html, Accessed October 3, 2004.

____. 2005b. *Defcon Forums- Ride and Room Sharing*. [Online] Available

   http://forum.defcon.org/archive/index.php/f-26.html, Accessed July 23, 2004.

Denning, D. E. 2001. Activism, hacktivism, and cyberterrorism: The Internet as a tool for

influencing foreign policy. Pp. 239-288 in Arquilla, J. and Ronfeldt, D. (Eds.) *Networks and*

Netwars: The Future of Terror, Crime, and Militancy. Santa Monica, CA: Rand.

Department of Justice. 2002a. *CHIP (Computer Hacking And Intellectual Property) Fact Sheet.*

[Online] Available http://www.usdoj.gov/criminal/cybercrime/chipfact.htm, Accessed

November, 20, 2004.

____. 2002b. *Operation Buccaneer: The Operation.* [Online] Available

http://www.usdoj.gov/criminal/cybercrime/ob/OBinvest.htm, Accessed November 15, 2004.

DiMaggio, P. and Powell, W. 1991. Introduction. Pp. 1-38 in Dimaggio, P. and Powell, W. (Eds.)

The New Institutionalism in Organizational Analysis. Chicago, IL: University of Chicago

Press.

Electronic Freedom Foundation. 2005. *About EFF*. [Online] Available http://www.eff.org/about/,

Accessed August 5, 2004.

Fiery, D. 1994. *Secrets of a Super Hacker.* Port Townsend, WA: Loompanics Unlimited.

Fishman, S., Rodenrys, K. and Schink, G. 1986. The Income of Organized Crime. Pp. 413-494 in

President's Commission on Organized Crime *The Impact: Organized Crime Today.*

Washington, DC: U.S: Government Printing Office.

Foster, J. 1990. *Villains: Crime and community in the inner city.* London: Routledge.

Furnell, S. 2002. *Cybercrime: Vandalizing the Information Society*. Boston, MA: Addison-

Wesley.

Garfinkel, H. 1967. *Studies in Ethnomethodology.* Englewood Cliffs, NJ: Prentice Hall.

Gibson, W. 1983. *Neuromancer.* New York: Ace Books.

Gilboa, N. 1996. Elites, Lamers, Narcs and Whores: Exploring the Computer Underground. Pp. 98-113 in Cherny, L. and Weise, E.R. (Eds.) *Wired women: Gender and new realities in cyberspace.* Seattle, WA: Seal Press.

Grabowski, P. and Smith, R. 2001. Telecommunications fraud in the digital age: The convergence of technologies. Pp. 29-43 in Wall D. S. (Ed.) *Crime and the Internet.* New York: Routledge.

Hamelink, C.J. 2000. *The Ethics of Cyberspace.* London: Sage.

Hamm, M. S. 1993. American Skinheads: The Criminology and Control of Hate Crime. Westport, CT: Praeger.

Hammersley, M. and Atkinson, P. 1983. *Ethnography: Principles in practice*. London: Tavistock.

Herbert, S. 1998. Police subculture reconsidered. *Criminology* 36 (2): 343-369.

Herring, S.C. 2004. Computer-mediated discourse analysis: An approach to researching online behavior. Pp. 338-376 In Barab, S.A., Kling, R., and Gray, J.H. (Eds.) *Designing for Virtual Communities in the Service of Learning.* New York: Cambridge University Press.

Holt, T. J. 2003. Examining a Transnational Problem: An Analysis of Computer Crime Victimization in Eight Countries From 1999 to 2001. *International Journal of Comparative and Applied Criminal Justice* 27 (2): 199-220.

The Honeynet Project. 2001. *Know your enemy: Learning about security threats.* Boston, MA: Addison-Wesley.

Jacobs, B.A. 1999. *Dealing Crack: The Social World of Streetcorner Selling*. Boston, MA: Northeastern University Press

Jargon File Version 4.4.6. [Online] Available http://www.catb.org/~esr/jargon/html/H/hacker.html, Accessed October 28, 2003.

Jordan, T. and Taylor, P. 1998. A sociology of hackers. *The Sociological Review* 46(4): 757-780.

____. 2004. *Hacktivism and Cyberwars: Rebels With a Cause.* New York: Routledge.

Katz, J. 1988. *Seductions of Crime: Moral and Sensual Attractions in Doing Evil.* New York: Basic Books.

Keller, L.S. 1988: Machismo and the hacker mentality: Some personal observations and speculations. Pp. 66-71. In Lovegrove, G. and Segal, B. (eds) *Women into Computing: Selected Papers 1988-1990.* New York: Springer-Verlag,

Kleen, L. J. 2001. *Malicious Hackers: A Framework for Analysis and Case Study.* (Master's Thesis, Air Force Institute of Technology, 2001). [Online] Available http://www.iwar.org.uk/iwar/resources/usaf/maxwell/students/2001/afit-gor-ens-01m-09.pdf, Accessed January 3, 2004.

Kornblum, W. 1997. *Sociology in a changing world 4th Edition.* Fort Worth, TX: Harcourt Brace and Company.

Landreth, B. 1985. *Out of the Inner Circle.* Washington: Microsoft Press.

Lemos, R. 2003. *Microsoft to offer bounty on hackers.* [Online] Available http://news.com.com/21007355_3-5102110.html?tag=nefd_top, Accessed November 15, 2003.

Levy, S. 1984. *Hackers: Heroes of the Computer Revolution.* New York: Dell.

Littman, J. 1997. *The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen.* New York: Little Brown.

Lofland, J. and Lofland, L. H. 1995. *Analyzing social settings: A guide to qualitative observation and analysis.* Belmont, CA: Wadsworth Publishing Company.

Loper, D. K. 2000. The criminology of computer hackers: A qualitative and quantitative analysis. (Doctoral Dissertation, Michigan State University, 2000) *Dissertation Abstracts International.* Volume: 61-08, Section: A, page: 3362.

McIntosh, M. 1975. *The Organization of Crime*. London: Macmillian.

Mann, D. and Sutton, M. 1998. Netcrime: More Change in the Organization of Thieving. *British Journal of Criminology* 38 (2): 201-229.

Matsueda, R. L., Gartner, R., Piliavin, I., and Polakowski, M. 1992. The prestige of criminal and conventional occupations: A subcultural model of criminal activity. *American Sociological Review* 57: 752-770.

Maurer, D.W. 1974. *The American confidence man.* Springfield, IL: Thomas.

Maxfield, M. G. and Babbie, E. 1998. *Research Methods for Criminal Justice and Criminology, 2nd Edition.* Belmont, CA: Wadsworth Publishing Company.

McCarthy, B. and Hagan, J. 2001. When crime pays: Capital, competence, and criminal success. *Social Forces* 79: 1035-1059.

MENA Business Reports. 2002. *Hacktivism: Pro-Islamic hacker groups joining forces globally.* [Online] Available http://web.lexis-nexis.com/universe/document?_m=a8bea342a9f5 6689f3986fa946c79f76&_docnum=3&wchp=dGLbVtb-zSkVA&_ md5=87f67b999724f1f411e93cee5da58d7f, Accessed April 30, 2004.

The Mentor. 1986. *The conscience of a hacker*. [Online] Available http://www.wbglinks.net/pages/reads/misc/hackersmanifesto.html, Accessed October 5, 2003.

Meyer, G. R. 1989. *The social organization of the computer underground.* (Masters Thesis, Northern Illinois University, 1989). [Online] Available http://csrc.nist.gov/secpubs/hacker.txt, Accessed December 29, 2003.

Miller, G. 1978. *Odd Jobs*. Englewood Cliffs, NJ: Prentice Hall.

Miller, J., Maxson, C.L., and Klein, M.W. 2001. *The Modern Gang Reader*, 2nd Edition. Los Angeles, CA: Roxbury Publishing Company.

Miller, W. B. 1958. Lower class culture as a generating milieu of gang delinquency. *Journal of Social Issues*, 14: 5-19.

Miles, M. and Huberman, A. 1984. *Qualitative Data Analysis*. London: Sage.

Mitnick Security Consulting, LLC. 2005. *Company Overview*. [Online] Available at http://www.mitnicksecurity.com/company.php, Accessed March 24, 2005.

Moore, D.W. 1995. *The Emperor's Virtual Clothes: The Naked Truth about Internet Culture*. Chapel Hill, NC: Algonquin books.

Morselli, C. and Tremblay, P. 2004. Criminal achievement, offender networks and the benefits of low self control. *Criminology* 43 (3): 773-804.

Noblett, M. G., Pollitt, M. M., Presley, L. A. 2000. Recovering and Examining Computer Forensic Evidence. Forensic Science Communications 2 (4). [Online] Available http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm, Accessed February 4, 2005.

Norman, P. 2001. Policing "high tech" crime within the global context: The role of transnational policy networks. Pp. 184-194 in Wall D. S. (Ed.) *Crime and the Internet.* New York: Routledge.

Office of Personnel Management. 2004. *Scholarship For Service: What is SFS?* [Online] Available http://www.sfs.opm.gov/ScholarshipMain.asp, Accessed April 13, 2005.

Parsons, T. 1937. *Structure of Social Action.* New York: McGraw-Hill.

Penetration Testing Guide. 2004. [Online] Available http://www.penetration-testing.com/, Accessed November 26, 2004.

Robinson, M. 1984. *Groups.* New York: John Wiley and Sons.

Rotundo, E. A. 1998. Boy Culture. Pp.337-362 in Jenkins, H. (Ed.) *The Children's Culture Reader*. New York: NYU Press.

Saint Louis Chapter 2600. 2003. *Part 2.* [Online] Available http://www.wearehope.com/, Accessed
　　　August, 24, 2003.

Schell, B.H., Dodge, J.L., with Moutsatsos, S.S. 2002. *The Hacking of America: Who's Doing it,*
　　　Why, and How. Westport, CT: Quorum Books.

Shimomura, T. and Markoff, J. 1996. *Takedown: The Pursuit and Capture of Kevin Mitnick,*
　　　America's Most Wanted Computer Outlaw-by the Man Who Did It. New York: Hyperion.

Short, J. F. 1968. Introduction. Pp.7-16 in Short, J.F. (Ed.) *Gang Delinquency and Delinquent*
　　　Subcultures. New York: Harper and Row.

Short, J. F. and Strodbeck, F. 1965. *Group Process and Gang Delinquency.* Chicago, IL:
　　　University of Chicago Press.

Silverman, D. 2001. *Interpreting Qualitative Data: Methods for Analysing Talk, Text, and*
　　　Interaction, 2nd Edition. Thousand Oaks, CA: SAGE Publications.

Simmons, J.L. 1985. The nature of deviant subcultures. Pp. In Rubington, E. and Weinberg, M.S.
　　　(Eds.) *Deviance: The interactionist perspective.* New York: Macmillan.

Slatalla, M. and Quittner, J. 1995. *Masters of deception: The gang that ruled cyberspace.* New
　　　York: Harper Collins Publishers.

Steffensmeier, D. J. 1986. *The Fence: In the Shadow of Two Worlds.* Totowa, NJ: Rowman and
　　　Littlefield.

Sterling, B. 1992. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier.* New
　　　York: Bantam.

Sykes, G. M. and Matza, D. 1957. Techniques of Neutralization. *American Sociological Review* 22:
　　　664-670.

Taylor, P.A. 1999. *Hackers: Crime in the digital sublime.* New York: Routledge.

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

Thomas, D., and Loader, B. D. 2000. Introduction- cybercrime: law enforcement, security, and surveillance in the information age. Pp.1-14 in Thomas, D. and Loader, B.D. (Eds.) *Cybercrime: Law enforcement, security and surveillance in the information age*. New York: Routledge.

Turkle, S. 1984. *The Second Self: Computers and the Human Spirit.* New York: Simon and Schuster.

U.K. National Computing Centre. 1994. *IT Security Breaches Survey Summary*. Manchester, U.K.: National Computing Centre.

Voiskonsky, A.E., Babaeva, J.D., and Smyslova, O.G. 2000. Attitudes towards computer hacking in Russia. Pp. 56-84 in Thomas, D. and Loader, B.D. (Eds.) *Cybercrime: Law enforcement, security and surveillance in the information age.* New York: Routledge.

Wall, D.S. 1999. Cybercrimes: New wine, no bottles? In Davies, P., Jupp, V., and Francis, P. (Eds.) *Invisible Crimes.* London: Macmillan.

Wall, D.S. 2001. Cybercrimes and the Internet. Pp. 1-17 in Wall D. S. (Ed.) *Crime and the Internet.* New York: Routledge.

Warr, M. 2002. *Companions in Crime: The Social Aspects of Criminal Conduct*. New York: Cambridge University Press.

Webopedia. 2003. *Wardriving.* [Online] Available http://www.webopedia.com/TERM/W/wardriving.html, Accessed April 4, 2005.

Williams, M. 2004. Understanding King Punisher and His Order: Vandalism in a Virtual Reality Community: Motives, Meanings and Possible Solutions. *Internet Journal of Criminology*.   [Online] Available

http://www.internetjournalofcriminology.com/Williams%20%20Understanding%20King%20Punisher%20and%20his%20Order.pdf, Accessed May, 04, 2005.

Williams, P. 2001. *Russian organized crime, Russian hacking, and U.S. security.* [Online] Available http://www.cert.org/research/isw/isw2001/papers/Williams-06-09.pdf, Accessed November 20, 2003.

Wolf, D. R. 1991. *The Rebels*. Toronto: University of Toronto Press.

Wolfgang, M. E., and Ferracuti, F. 1967. *The subculture of violence: Towards an integrated theory in criminology*. London: Tavistock Publications.

Woo, H. J. 2003. The hacker mentality: Exploring the relationship between psychological variables and hacking activities. (Doctoral Dissertation, The University of Georgia, 2003)

Dissertation   Abstracts International. Volume: 64-02, Section: A.

Wood et al. 1997. Nonsocial Reinforcement and Habitual Criminal Conduct: An Extension of Learning Theory. *Criminology* 35: 335-366.

Wright, R. T. and Decker, S. H. 1994. *Burglars on the job: Streetlife and residential break-ins*. Boston, MA: Northeastern University Press.

Wysocki, M. D. 2003. Cracking the hacker code: An analysis of the computer hacker subculture from multiple perspectives. (Doctoral Dissertation, Northwestern, 2003) *Dissertation Abstracts International.* Volume: 64-04, Section: A, page: 1125.

Zimmerman, D.H. and Wieder, D. L. 1977. You Can't Help but Get Stoned. *Social Problems* 25: 198-207.