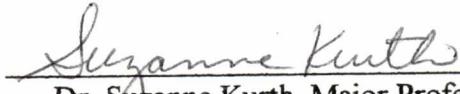
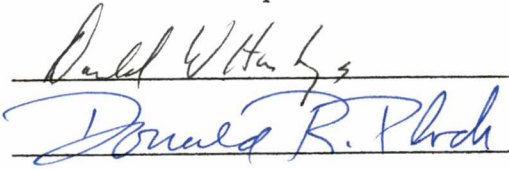


To the Graduate Council:

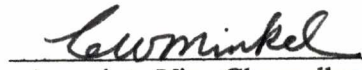
I am submitting herewith a thesis written by Sean Thomas Huss entitled "Hackers: Practices, Motivations, and Identity." I have examined the final copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Arts, with a major in Sociology.


Dr. Suzanne Kurth, Major Professor

We have read this thesis and
recommend its acceptance:



Accepted for the Council:


Associate Vice Chancellor and
Dean of the Graduate School

HACKERS: PRACTICES, MOTIVATIONS, AND IDENTITY

A Thesis
Presented for the
Master of Arts
Degree
The University of Tennessee, Knoxville

Sean Thomas Huss
May 1998

Copyright © Sean Thomas Huss, 1998
All rights reserved

ACKNOWLEDGMENTS

I wish to thank my advisor and committee chair, Dr. Suzanne Kurth, for the consistent direction and encouragement that she provided throughout the course of this investigation. Dr. Kurth's revisions of the initial drafts well past the end of the Fall 1997 semester demonstrated her dedication and support, and I feel safe in saying that without her this project would not have been completed. I also wish to thank my other committee members Dr. Donald Hastings and Dr. Donald Ploch. Dr. Hastings's constant enthusiasm and coaching in both methods for analysis and organizing the data contributed greatly to this project. Dr. Ploch's comments, interest, and help with resources added depth that directed this project greatly. I have enjoyed working with all of my committee members, and I only hope that this project lives up to their contributions.

I would also like to thank my family and several persons in the department of sociology without whom this project would not have been possible. I would like to thank my parents (Tom and Gail Huss) and my sister (Kristen McCauley) who supported my endeavors by traveling with me to Las Vegas, Nevada, and serving as research assistants for content analyses of news reports. Their financial, emotional, and coding support was invaluable, and without them much of the data would not have been collected. I would like to thank Dave Harrison who accompanied me to New York City and provided me with a place to stay. Dave served as an invaluable research assistant in the collection of survey responses, and served as a true friend in his help to this project. I would like to thank Kent Kerley, Brent Marshall, Heith Copes, Andy Hochstetler, Karen Mason, and Todd Matthews all of whom I consider friends that contributed to many aspects of this project whether or not they are aware of it. Finally, I would like to thank Pam and Shirley who demonstrated amazing patience in helping me format the survey instrument.

ABSTRACT

The computer nerd image of the individual who spends long hours mastering computer systems is being challenged by the image of a computer hacker, a deviant who violates organizational rules to access systems, and the even more negative image of the computer criminal, a person who financially profits from entering systems or maliciously harms systems. Drawing on observations from two hacker conventions, 15 on-line interviews with hackers, threads on two list-servers pertaining to hackers' perceptions of their activities (October 1996 to September 1997), and survey data from 182 self-defined hackers, hackers' views of their activities, their contributions to the field of computing, unethical computing behavior, and themselves are derived. These images or views are compared with those promoted by computer security professionals, the computer industry, and law makers, as well as those which appear in the mass media. The role of a computer underground or subculture in defining hacking is evaluated.

TABLE OF CONTENTS

CHAPTER	PAGE
I. INTRODUCTION, THEORY, AND LITERATURE REVIEW	1
Theoretical Framework	3
Social Categorization and Identity	4
Deviant Careers, Subcultures, and Stigma Management	6
General Questions	9
Literature Review	9
Defining Hackers and Hacking	10
The Computer Security Perspective	13
The Computer Underground and The Hacker Ethic	18
Criminalization of Hacking	20
Discussion on Literature	26
II. METHODS	28
Difficulties in Gaining Acceptance from Hackers	28
Sample	29
Techniques	31
Measures	34
Scales and Reliability	35
Statistical Analyses	40
Sample Characteristics	41
III. HACKERS AND THE MASS MEDIA	42
Mass Media Portrayals of Hackers	43
Hackers' Views on the Media	48
Hackers' Perceptions of Hackers and Hacking	54
Definitions of Hackers and Hacking	54
Experiences and Beliefs	56
Motivations	60
Activities	61
Exaggerations and Media Accounts	67
Discussion	68
IV. THE HACKER IDENTITY	72
Identity Development and Interaction	72
Identity Importance and Commitment	80
Typology of Hackers and Identity Management	84
Discussion	87

VI. CONCLUSIONS AND FUTURE RESEARCH	91
Summary	91
Conclusions	92
Problems to Address and Future Research	95
REFERENCES	97
APPENDICES	105
Appendix One: Media Sources for Content Analyses	106
Appendix Two: Content Analysis Coding Sheet	113
Appendix Three: Survey Instrument	123
Appendix Four: Qualitative Questions	132
VITA	137

LIST OF TABLES

TABLE		PAGE
1	Communalities and Maximum Likelihood Rotated Factor Loadings for Motivational Scales of Self-Identified Hackers	38
2	Communalities and Maximum Likelihood Rotated Factor Loadings for Self-Report Scales of Self Identified Hackers	39
3	Percentage Distributions for Statements Regarding the Fairness of Printed and Television News Reports	51
4	Percentage Distributions for Perceived Influence of Media Sources and Hacker Sources on Law Makers' and the General Public's Perceptions	53
5	Percentage Distributions for Statements on Computer Crime Laws and Lack of Understanding of Law Enforcement	59
6	Percentage Distributions for Importance of Motivations in Hacking Activities	62
7	Percentage Distributions for Unauthorized Access/Alteration Activities Over the Six Month Period Prior to Completing the Survey	63
8	Percentage Distributions for Electronic Theft Activities Over the Six Month Period Prior to Completing the Survey	64
9	Percentage Distributions for Deliberate Damage Activities Over the Six Month Period Prior to Completing the Survey	65
10	Percentage Distributions for Software Piracy Activities Over the Six Month Period Prior to Completing the Survey	65
11	Pearson Product Moment Correlation Coefficients Matrix of Self-Reported Activities Scales	66
12	Percentage Distributions for Hackers' Perceived Publicity Seeking and Exaggerated Claims Making Behavior	68

TABLE		PAGE
13	Pearson Product Moment Correlation Coefficients Matrix of Length of Time Hacking and Activity Scales	79
14	Serious Activities by Length of Time Hacking	80
15	Percentage Distributions of Importance of Hacker Identity	81
16	Percentage Distributions of Time and Money Spent in Non-Job Related Hacker Activities	81
17	Pearson Product Moment Correlation Coefficients Matrix of Identity Importance, Commitment, and Motivation Scales	83
18	Effects of Age, Importance of Identity, and Commitment to Hacking on Motivational Scales for Hackers	83
19	Percentage Distributions on Secrecy of Hackers	86

CHAPTER ONE

INTRODUCTION, THEORY, AND LITERATURE REVIEW

The computer is the hallmark of technological development for the second half of the twentieth century; its social consequences are controversial. The widespread use of computers generates questions about dependence on computer systems and the vulnerability of the vast quantities of information stored in those systems. The questions are addressed in opposing ways by two sets of persons vitally interested in access to computer systems. On the one hand, computer security professionals and law makers assert that those who unofficially enter computer systems are criminals. Their rhetoric invokes norms and values related to the sanctity of private property and information, and demonizes computer hackers as a threat to them. On the other hand, those who hack systems argue that computer security professionals are handmaidens of an economic order that denies citizens such as themselves freedom of information by invoking the less than fundamental right to private property. Their rhetoric contrasts a corporate model emphasizing property rights with a model emphasizing the public good devolving from a free flow of information. At one level, the debate focuses on conflicting rights (information and property); on another it focuses on the social identity of those who hack computer systems.

The debate is played out in the mass media. The prototypical computer crime story presents a hacker who is a maladjusted, teenage, computer genius who is a thrill seeker that breaks into a military computer system and brings humanity to the brink of World War III. Mass media portrayals often imply that hackers are responsible for most types of computer crimes. Hackers dispute the negative media images which stigmatize of them as some form of computer criminal (Denning, 1990). Some media accounts present a more balanced picture. Journalist Bruce Sterling (1992) reports that many self-defined

hackers are mature, law abiding, hard working individuals performing cutting edge work in the area of electronics. Some of them influence the development of technologies by challenging the status quo of the electronic community (Sterling, 1992). Yet, such reporting seems to be the exception rather than the rule.

Hackers distinguish their activities from those presented in most mass media portrayals by emphasizing motivations (Denning, 1990; Fiery, 1994). Typically, hackers claim to be motivated not by financial need or revenge, but rather by belief in the free dissemination of information and desire for intellectual challenge. They argue that their use of computers is guided by a code of ethics developed by computer pioneers. In their statements (e.g., online, in books, at meetings) hackers invoke an ethic of free access to information and intellectual challenge, and the right to engage in acts, illegal or not, in their pursuit of information and challenge. For them, the difficult to discern distinction between an ethically motivated hack and an intrusion with criminal intent is what separates hackers and computer criminals (Fiery, 1994). Hackers portray computer criminals as those who commit offenses which harm computer systems or provide financial gain; hackers are people seeking challenge and knowledge (Best and Luckenbill, 1994; Fiery, 1994).

Hackers argue that media portrayals ignore issues posed by commercial development in the electronic community. First, the treatment of information as a commodity challenges conventional conceptions of trespass, theft, invasion of privacy, and property rights. Second, the centralization of computer systems and restriction of access to all forms of information represent the domination of a particular corporate model. When computer security professionals counter that hackers' activities are costly and violate professional ethics in the electronic community (codified in computer crime law), hackers respond that the costs generated by their electronic intrusions are minimal

compared with those associated with "real" criminal activity (Denning, 1990; Hollinger and Lance-Kadduce, 1988).

Hackers deserve sociological attention, for as the use and importance of computer technology grow, so does the controversy associated with hackers and their activities. But limited sociological research addresses the nature of computer crime or hacking, and most information about them comes from the mass media (Bequai, 1978; Collier and Spaul, 1992; Forester and Morrison, 1990; Hollinger, 1993; Hollinger and Lance-Kadduce, 1988; Meyer, 1989). This thesis is an exploratory study of the practices, motivations, and identities of self defined hackers. Observations from two hacker conventions, 15 online interviews with hackers, threads on two list-servers pertaining to hackers' perceptions of their activities (October 1996 to September 1997), and survey data from 183 self defined hackers are used to derive hackers' views of hacking activities, their contributions to the field of computing, unethical computing behavior, and their identities. These images or views are compared with those promoted by computer security professionals and the mass media. The role of a computer underground or subculture in defining hacking is also evaluated.

Theoretical Framework

To develop a framework for investigating the practices, motivations, and identities of hackers, I draw on various theoretical perspectives. Interactionist theories on the nature of categorization, identity, and groups provide a basis for exploring hackers and hacking. The labeling perspective emphasizes the stages through which neophytes may pass in becoming hackers. Theories on stigma and its management point to the potential techniques for the reduction of stigma of labeled individuals. In addition, subcultural theories on deviance direct attention to norms and the process of value conveyance.

Social Categorization and Identity

Social interaction involves the transmission of both implicit and explicit information. This information is made meaningful through the use of social categories and types (Goffman, 1963; McCall and Simons, 1966). These social categories are based on arbitrary distinctions with those objects or persons in a category assumed to share common attributes (Goffman, 1963). Social categories provide frameworks with which evaluations may be made of individuals and the consistency of their behavior to social expectations. Those individuals whose behavior is believed to be inconsistent may be considered different and labeled outsiders (Becker, 1963; Goffman, 1963). Evaluations of categories are based on both normative expectations and the values associated with experiences of these categories (Strauss, 1997). The normative expectations associated with categories provide a framework for engaging in action and interpreting others' action. Values may also direct action based on experience with a category (Strauss, 1997). Values involve relational experiences between perceivers and perceived categories which take the forms of judgments guiding future perceptions of a category (e.g., bad/good, law abiding/criminal) (Klapp, 1962; Strauss, 1997).

Categories which serve as the foundation for social and personal identification are based on existing symbols and images (Klapp, 1962; Rubington and Weinberg, 1973). This stock of social types provides the framework for judgments of self and others (Klapp, 1962; Rubington and Weinberg, 1973). These linkages allow for the identification of models and motivations for behaviors in role performance (Klapp, 1962; Rubington and Weinberg, 1973). Such models serve as the foundation for the construction of individual and group identities (Klapp, 1962; Rubington and Weinberg, 1973). Use of social types allows for the definition of new categories, linking emergent forms of behavior with acceptable forms of behavior defined in the existing social structure (Klapp, 1962; Rubington and Weinberg, 1973). Social types also allow for the delineation of informal

role structures and identification of those typed as outside of the mainstream (Klapp, 1962; Rubington and Weinberg, 1973).

Examples of broader social types are heroes and villains (Klapp, 1962). Heroic types have attributes more commonly associated with the social types *winner* and *independent spirit* (Klapp, 1962:27). The *winner* social type is further subdivided into the *brain* and the *smooth operator* (Klapp, 1962:31-33). Brains are known for their ability to win through demonstrations of their intellect and technical abilities (Klapp, 1962). Most often, brains are acknowledged as heroes, if they exhibit both power through ability to bring about social changes and understand the implications of their power (Klapp, 1962). Smooth operators are known for their ability to manipulate others in complex games in which competition and winning are the goals (Klapp, 1962). They exploit opportunities in ambiguous contexts, and are considered heroic if they deceive those capable of preventing exploitation (Klapp, 1962). The social type of independent spirit exhibits attributes of strong individuality and can take a stance alternative to the mainstream (Klapp, 1962). They are most often considered heroes, if their individuality is expressed in the accomplishment of some goal which necessitates deviation from the norm (Klapp, 1962).

Unlike heroic types, villainous types have attributes which threaten or intrude on the social order (Klapp, 1962). They may be divided into three general classes: *desperadoes*, *rebels*, and *strangers* (Klapp, 1962). Desperadoes use extreme means to disrupt social order in various contexts (Klapp, 1962). Rebellious types are representative of individuals attacking existing authority structures. The social type strangers includes individuals who threaten the unity and security of groups (Klapp, 1962). Such attributes also include the alternative nature of groups or individuals perceived to be outside of the mainstream and therefore not to be trusted (Klapp, 1962).

Individuals may be assigned to categories, typed or labeled by others, or they may embrace such role identities (Becker, 1963; Klapp, 1962). Labeling is most often based

on the interpretation and judgments of others using attributes expressed in the character or behavior of individuals or groups (Becker, 1963). Identity construction reflects the desire of particular individuals to model their behaviors on attributes consistent with social types they consider to be salient to the information they wish to convey about themselves to others (Klapp, 1962). Both labeling processes and identity construction demonstrate how categories have an impact on how individuals view themselves through interaction with others (Becker, 1963; Goffman, 1963; Klapp, 1962; Lemert, 1967). Sociologists recognize that some social types are perceived as deviant and may be drawn on to categorized persons through either self or societal selection (Becker, 1963; Goffman, 1963; Klapp, 1962; Lemert, 1967).

Deviant Careers, Subcultures, and Stigma Management

Whether individuals or groups are labeled as deviant varies with the availability of social types in public consciousness and discourse, as well as the visibility of their behaviors (Becker, 1963; Klapp, 1962). Social types and behaviors associated with them are brought to public attention through the mass media. Interest groups may play a central role in labeling certain attributes or behaviors as deviant and establishing sanctions created through societal reaction to attributes or behaviors (Becker, 1963; Klapp, 1962). Societal reactions are manifested as socially manufactured rules and applied to individuals through the labeling process (Becker, 1963).

Individuals may construct deviant identities regardless of potential consequences. Individuals may identify with deviant categories and attributes associated with them (Klapp, 1962). The individual may seek others with similar interests who are constructing similar deviant identities (Becker, 1963; Klapp, 1962). Fundamentally, this process of constructing a deviant identity draws on attributes learned through public discourse or social interaction (Klapp, 1962).

The construction of a deviant identity may be understood as an outcome of pursuing a "deviant career" (Becker, 1963). A deviant career begins with an act which is perceived to break a set of rules advocated by a social or interest group (Becker, 1963). Whether an infraction is intentional or unintentional, if it is perceived to occur, it will result in a response (Becker, 1963). If the act is seen as representative of the person, the individual becomes typecast, identified as deviant (Becker, 1963). Responses from social control agents lead to a deviant public identity which, in turn, generates new expectations and treatment from the general public (Becker, 1963). The label leads others to limit contact with the person labeled deviant, and eventually lead the person labeled to accept a new identity (Becker, 1963). In other instances, the individual is not the passive object of labeling but rather an active agent pursuing a deviant identity. In any case, in the final stage of the career the individual begins to associate with a deviant group or subculture and internalize new (deviant) expectations based on interactions with others in the subculture (Becker, 1963).

Interactions with similar others provide a context in which individuals may engage in deviant activities and receive reinforcement for such activities (Becker, 1963). These interactions may produce a shared set of symbols and beliefs, a subculture. Subcultures have distinct vocabularies, beliefs, and norms, and forms of interaction between members (McCaghy and Capron, 1994). These components provide the framework through which behavior is facilitated or sanctioned consistent with subcultural norms and values. Through interactions in subcultures, members are provided knowledge, techniques, values, and beliefs, as well as appropriate frameworks for action (Agnew, 1995; McCaghy and Capron, 1994). In some instances, these frameworks for action are based on existing values or beliefs but in exaggerated form (Matza and Sykes, 1961).

Subcultures may also provide techniques for neutralizing guilt and justifications for further deviant behaviors. Individuals may adopt techniques to neutralize the guilt

associated with actions perceived to be deviant: denial of responsibility, a denial of injury, a denial of the victim, and condemnation of the condemners (Sykes and Matza, 1957). Justifications may be based on exaggerated values, if these values are perceived to be important by others in the larger social system (Benson, 1985). After they have adopted subcultural beliefs, individuals offer justifications (reasons) for actions despite their perceived negative qualities in the larger culture (Benson, 1985). Techniques of neutralization allow individuals to reduce the potential internal conflict over engaging in the deviant activity (for violating overriding systems of norms), to engage in activities perceived to be deviant, and to manage potential social stigma.

Stigma is derived from social judgments of categories based on perceived attributes of physical and character flaws, as well as attributes such as ethnicity or religion (Goffman, 1963). Perceived flaws serve as the basis for categorization, and range from immediately observable (i.e., ethnic or physical attributes) to ones not immediately observable (i.e., alcoholism or criminal history) (Goffman, 1963). Those with visible stigmata are discredited; those whose attributes are not immediately observable are discreditable (Goffman, 1963). The discreditable maintain greater control over social information, as opposed to the discredited who have less control (Goffman, 1963).

Stigmatization results from the categorization process, and is a defining process for an individual's self. A discrepancy may exist between the attributes an individual may be proved to possess (actual social identity) and the attributes assigned by others retrospectively (virtual social identity) (Goffman, 1963). The difference between virtual and actual social identities reflects the symbolic information an individual conveys in interaction (Goffman, 1963). For the discreditable, contradictions may cast doubt on the validity of the information they convey, and may result in spoiled social identities (Goffman, 1963).

People engage in forms of stigma management (i.e., the control of information about selves) at both individual and group levels (Goffman, 1963). Stigma also may be managed through group alignments in two ways. First, individuals may distinguish themselves from others in the deviant category by pointing to and sanctioning in-group behaviors inconsistent with the category (Goffman, 1963). Second, individuals may draw on frameworks for the management of their deviant identity learned through interactions with others in their deviant category (Goffman, 1963). Both techniques reflect an stigmatized individuals' perception of the stigma and the advice offered by others so stigmatized (Goffman, 1963).

General Questions

The blending of these perspectives provides a framework to raise several general question about the practices, motivations, and identities of hackers. First, to what extent are hackers labeled by the mass media? Second, how accurate are media portrayals of hackers? Third, to what extent do mass media portrayals contribute to the meaning of the hacker identity for hackers? Finally, what is the career path of a hacker and what techniques do hackers use to control the meanings of their image? To address these questions, the complex relationships among computer security professionals, hackers, and the mass media are addressed in chapter three. Chapter four presents an analysis of the career path of the hacker, attachment to the hacker identity, and techniques of stigma management. Before proceeding to methods and analysis chapters, definitions of and issues related to hackers and hacking are presented in a literature review.

Literature Review

Relevant literature is reviewed first by focusing on the history and evolution of the conceptions of hackers and hacker activities. Next, the perspective of computer security professionals and research addressing issues raised by it are reviewed. Then research on the computer underground, hackers, and information sharing is presented. Next, the role

of the media in shaping public perceptions of hacking as a form of deviance, and research on the images of hackers in the mass media are used to analyze central issues in the hacker-mass media relationship. Finally, relevant research is discussed, and the research questions directing this project are presented.

Defining Hackers and Hacking

Formerly referring to one who makes furniture with an ax, a prankster, or an amateur golfer, the term hacker is now linked to people facile in the use of computer technologies (Chandler, 1997; Raymond and Steele, 1996). The terms hacker and hacking have a range of meanings that focus on cleverness in computer programming (Forester and Morrison, 1994). *The New Hacker's Dictionary* provides eight definitions of the term hacker as follows:

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users.
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** (*the reason or motivation for expending effort toward a seemingly useless goal...the accomplished goal is a hack*).
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'.
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 is cracker. (Raymond and Steele, 1996:218)

Being identified as a hacker may signify membership in a loosely organized group or community which awards status based on the level of computer skill, and subscribes to

some form of the hacker ethic (Raymond and Steele, 1996). Some of the variation in definitions reflects diversity in the behavior of those called hackers.

The activities of successive generations of computer users played an important role in the evolution of the term (Chandler, 1996). The first hackers of the late 1960s and early 1970s were perceived to be technological wizards guided by principles of sharing information and electronic exploration (Chandler, 1996; Hafner and Markhoff, 1995, Clough and Mungo, 1992). For these early enthusiasts the term hacker served as a positive label of accomplishment. A second wave of hackers (e.g., Stephen Wozniack and Stephen Jobs of Apple) actively participated in the personal computer revolution of the early 1980s (Chandler, 1996; Clough and Mungo, 1992; Hafner and Markhoff, 1995; Rheingold, 1991). The label hacker served as a positive label of accomplishment and the potential for economic success for this second wave (Chandler, 1996; Clough and Mungo, 1992).

Modified meanings of hacker and hacking appeared with the third and fourth waves or generations of hackers. The third generation of hackers focused more on the pirating of software games and the creation of new games (Chandler, 1996; Clough and Mungo, 1992). For them, the term hacker referred to those engaging in software piracy or those engaged in complicated programming (more consistent with earlier conceptions) (Chandler, 1996). The denotation of illicit activities associated with software piracy emerged more strongly in the current (fourth) generation of hackers. These hackers publicly endorsed many of the founding principles of the first hackers, but certain activities (e.g., the creation and use of viruses) made them distinct from earlier hackers (Chandler, 1996; Clough and Mungo, 1992). Chandler (1996) concludes that this fourth generation led the mass media to redefine hackers and their activities as threatening or illegal.

The values and motives endorsed by successive generations of hackers are indicative of these shifts in meaning. The first wave of hackers claimed to be motivated by

the ideas of free dissemination of information and the pursuit of intellectual challenge through the use of computers. Pioneering computer scientists of the late 1960s and 1970s at MIT and Stanford laid the foundation for the "Hacker Ethic" (Levy, 1984). Their twofold purpose was the development and improvement of computer systems, an activity which they perceived necessitated unrestricted access to computer systems and software (Levy, 1984). The earliest hackers argued the necessity of committing deviant acts to gain access to restricted systems.

A second source for values is the Phone Phreaker movement of the early 1970s. Focusing specifically on the mastery of telephonic technologies, this group developed the Youth International Party Line newsletters aimed at defeating phone systems in what was claimed to be protest against the Vietnam War (BloomBecker, 1988; Sterling, 1992). The newsletter Technical Assistance Program (TAP) served as the progenitor of publications now found in the computer underground (Platt, 1997; Sterling, 1992). TAP made specialized information on subverting the phone system through the use of tonal frequencies widely available.

Both in the late 1970s and 1980s computer hacking and phreaking were transformed with the introduction of the micro computer and computer networks which made the phone system a means to an end rather than an end in itself (Platt, 1997). Micro computing systems enabled anyone with the time and knowledge to explore actively the intricacies of computer systems. The modem provided computer users with opportunities to exceed the limits of their own systems into the earliest forms of what later became the Internet, and to gain unauthorized access to external computing systems. In addition, these innovations dramatically expanded potential for information exchange.

With the infrastructure in place, micro computer users became the operating managers of sites allowing others to access and share information. These sites, known as Bulletin Board Systems (BBSes), grew from about 12 in 1978 and 50 in 1980 to

thousands today (Platt, 1997). The early years of BBS development provided the first opportunities for others to engage in activities consistent with the beliefs of the early hackers at MIT. Adept programmers known as Pirates would access the source code of computer games, remove the copy protection programs, and post the games on their BBS systems allowing others to download these games free of charge (Platt, 1997). BBSs also provided a forum for role-playing games hosted by the operator of the system. With names such as "Temple of Chaos," these boards contributed to the "anything goes" climate for hackers (Platt, 1997:19). Some hackers began to engage in activities with larger social consequences; they crashed systems and engaged in on-line competition to do so (Platt, 1997).

The lack of formal controls on computer usage was for hackers the equivalent of an "electronic Garden of Eden" (Platt, 1997:20). Few knew about these BBSs, and those who did were adept computer users. The criterion for status was the skill of the computer user. This environment contributed to a game playing atmosphere in which the evolution of viruses and crashing of systems became common. Hackers developed rivalries, taking names from comic book, role-playing, and literary characters (Platt, 1997). Viruses and other programs designed to crash systems were placed on BBS systems with the intent that others would download these programs, run them, and have to deal with the aftermath of a system crash. Some victims and law enforcement officials did not see these activities as game playing. Unrestricted activities in the electronic community came to an end when the media began reporting stories of hacking (Platt, 1997). These media accounts encouraged legislators to equate hacker with computer criminal.

The Computer Security Perspective

As the number of hackers grew, computer software companies and organizations dependent on their computer systems hired "security" people to protect their systems. Many of these computer security people were drawn from the ranks of hackers, for they

were the ones with the requisite knowledge. A computer security perspective on hackers and hacking emerged which focuses on three interrelated issues: 1) greater dependence on computer systems; 2) increases in the amount of information held in computer systems; and 3) development of ethical codes necessary to protect information and computer systems (Parker, 1983). Computer security specialists focus on individuals posing a threat to data and information, "system hackers" (Parker, 1983:183)

System hackers engage in a variety of activities, the least damaging of which is unauthorized access. Individuals who engage in "unauthorized system exploration" presumably are motivated predominantly by intellectual interests (Parker, 1983:131). Some in the computer security profession assert that such activities may be addictive (Parker, 1983). Hackers may forgo eating or sleeping to pursue their activities, and forego other goals and accomplishments for those obtained in the electronic world (Parker, 1983). Such individuals engage in their activities in isolation. The argument is that this obsession with computers matched with unrestricted, isolated computer activities may encourage individuals to engage in "unprincipled" activities free of immediately experienced consequences (Parker, 1983:133).

Computer security professionals argue hacking also may occur while learning computer systems from others (Parker, 1976, 1983). The behaviors of hackers are rooted in learning applications of computer technologies, a process in which peers and instructors may encourage them to commit deviant acts to demonstrate their expertise (Levy, 1984; Hollinger, 1993; Parker, 1976, 1983). Hackers learn computer use is an intellectual game in which the computer is a tool to achieve desired output, and potential normative infractions of the game are unimportant (Parker, 1976).

In the 1970s, such game playing was allegedly supported in university systems in that the importance of computer technologies and the threats to safety from unauthorized attacks were not stressed (Parker, 1976). Parker (1976, 1983) asserts that most academic

majors presented classes on their disciplines' ethical codes (e.g., business programs), but that computer science programs did not. Levy (1984) demonstrates that the early computer enthusiast's hacker mentality allowed for deviant behaviors (altering computer equipment and software, breaking into locked offices, and stealing equipment) which were tolerated by their professors and peers. Parker (1983) argues that the hacker ethic, which is consistent with game playing, is a justification for behaviors that are costly. Specifically, the hacker ethic may serve as justification for game playing in settings such as the work place (Parker, 1976, 1983). Parker (1976:48) concludes:

Until students are taught that the computer is a sacrosanct, important tool not to be played with in unauthorized fashion, we will continue to have a flow of new graduates coming into our businesses, government, and institutions prepared to continue their game playing, but where the stakes are real.

For Parker, this game playing mentality serves as a criminogenic factor in computer crimes.

Sociologist Richard Hollinger (1984, 1988, 1993) asks about the normative climate of computer use by presenting scenarios of computer crime to respondents. The first study (1984, 1993) of a sample of 200 undergraduate computer science majors presented scenarios and asked respondents to indicate their inclination for involvement in certain forms of computer crime. Hollinger reported that 10% of respondents indicated that they would be likely to commit acts such as vandalism, fraud, or embezzlement, and more than twice as many (22%) stated that they might examine or modify confidential information, if they had the opportunity. Only a few (3%) stated that they definitely would not commit such computer violations (Hollinger, 1984, 1993).

In a second study based on structured interviews with a sample of eight computer science students and apprehended computer criminals, Hollinger suggests involvement follows a linear path beginning with software piracy, followed by browsing and cracking activities (1984, 1993). The activities acknowledged did not differ for this small sample of

apprehended computer criminals and computer science students (Hollinger, 1984, 1993). In a third study (Hollinger, 1993), a sample of 1,672 college students received self report questionnaires which focused mainly on academic dishonesty, but included two computer related crime scenarios; software piracy and unauthorized access. The results indicated that piracy and unauthorized access are rare on this college campus, although a significant minority participated in software piracy (10.2%) and a smaller percentage gained unauthorized access to another person's account (3.4%) one or more times (Hollinger, 1993). Thus, Hollinger's results do provide some support for the claims of computer security specialists.

Some computer security specialists argue that hackers' willingness to engage in illegal activities may reflect an ethical position emphasizing the priority of freedom of information over the right to control information (Denning, 1990). Based on interviews with nine hackers ranging in age from 17 to 28, Denning (1990) identifies areas of concern to hackers related to their public image and freedom of information. Her interviewees state that despite the media generated image of hackers, they do not seek access to confidential, personal information and believe that such information should be secure (Denning, 1990). But they complain that the restriction of open access to computer systems and general information may be seen to represent the domination of a particular corporate model. A model they believe unduly restricts access to computer systems and prompts corporations to collect a great deal of questionable information on individuals (e.g., credit card spending habits) (Denning, 1990). Denning (1990) concludes that hackers express concern over a growing information gap which is inconsistent with a social responsibility to share knowledge and educate the public.

Subsequently, Denning (1995) interviewed law enforcement personnel and other computer security experts, and proposes that hackers' activities do not represent a debate over First and Fourth Amendment rights, but rather they are system intrusions. Hackers

often displace responsibility for their activities on systems administrators who make it easy for them to intrude without addressing their own responsibility for the intrusions and their role in the creation of opportunities for more serious criminal behavior (Denning, 1995). Drawing on a computer security perspective, Denning (1995) concludes that hackers may be a greater threat than they realize, and discussion should not focus on the ethical issues raised by hackers.

A few computer security specialists argue hackers do not pose a serious problem; their activities are more of a nuisance than a real threat (Winkler, 1997). The activities which pose a threat are those which may facilitate criminal activity by identifying weaknesses in systems (Winkler, 1997). For example, Winkler (1997) asserts that possibly 200 "computer geniuses" have the skill to discover vulnerabilities in systems, and an additional 1000 are capable of developing tools to exploit these weaknesses. Once information on these exploits is shared with the larger hacker community, this information becomes available to thousands of others who are the real threat in that they do not fully understand the systems they exploit, nor do they fully understand the techniques necessary to reduce the potential for harm to the systems (Winkler, 1997:86).

The "clueless" thousands are threats to computer systems in two ways. First, unskilled hackers may intentionally or unintentionally cause major damage to systems. Highly trained computer specialists often cause unintentional damage to systems when working on them, and that unskilled individuals unintentionally may cause even greater damage (Winkler, 1997). Unskilled hackers pose a second threat for they share information on their exploits to gain status in the hacking community. Many unskilled hackers may brag about their ability to enter systems and delete existing files (Winkler, 1997). The perceived need to demonstrate skill in the hacker community may make hackers striving for status in the community unwitting accomplices to more serious criminal behavior such as espionage or theft (Winkler, 1997).

Hard line computer security specialists argue that an intensive effort must be made to define the activities of hackers as unacceptable and criminal (Parker, 1983). They emphasize the need to address computer addiction, the sharing of information on systems, and the development of ethical codes and laws prohibiting hacking activities (Parker, 1983). Others argue that although stricter ethical codes may deter some from hacking, greater attention should be directed to security and the detection and prosecution of hackers (Denning, 1995; Winkler, 1997). They contend that the real threat of hackers is that if they are not deterred, the sharing of information on accessing systems may facilitate criminal behavior with greater consequences than unauthorized access (Denning, 1995; Winkler, 1997). Despite these variations on similar themes in the computer security perspective, hacking is defined as a serious problem whether or not criminal behavior occurs because of the opportunities it may provide for others to engage in criminal behavior perceived not to be serious.

The Computer Underground and The Hacker Ethic

Sociologist Gordon Meyer points to opportunities for the distribution of information on systems by hackers based on his analysis of the social organization of a deviant subculture, the computer underground. The computer underground is mostly a combination of hackers, phone phreakers, and software pirates (Meyer, 1989). The computer underground serves "primarily as a social network of individuals that perform their acts separately, yet support each other by sharing information and resources" (Meyer, 1989:11). More specifically, members of the computer underground are colleagues who share information facilitating deviant activities. Contacts often are made through Bulletin Board Services (BBSes) or list-servers (i.e., discussion groups that communicate through e-mail software packages) rather than face-to-face. Through this network of associations, information on techniques to enter secure systems, manipulate data, and avoid detection, as well as passwords or targets are exchanged (Meyer, 1989).

These interactions support a system of beliefs and ideology. Members of the underground learn the value of gaining illegal access to computer systems for the purposes of acquiring information and excitement (Meyer, 1989). Hackers learn that withholding information makes them subject to criticism from other members (Meyer, 1989). Members of the computer underground share justifications for their behaviors with their hacker ethic:

1. Access to computers--and anything which might teach you about the way the world works--should be unlimited and total. Always yield to the hands on imperative!
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 beauty on a computer.
6. Computers can change your life for the better.
(Levy, 1984:39-49):

This ethic provides justification for the commission of illegal computer acts which subvert the perceived authority of informational elites and aid in the quest for the acquisition of knowledge (Meyer, 1989).

The hacker ideology allows for the potential that certain information may not be shared. Participants in the computer underground see themselves not only as colleagues but also competitors in a world with a limited supply of "hackable" computer systems. The information shared usually is of a general nature (Meyer, 1989). When a hacker submits information on the weakness of specific systems, he or she may alert system operators and limit the number of times illegal access may be gained (Meyer, 1989). The more hackers accessing the system increases the likelihood of discovery, so that distribution of too much information may result in sanctions from other hackers.

In addition to information exchange, this network provides a framework for interpreting experiences and the transmission of norms and values (Best and Luckenbill, 1994). The core tenets of the hacker ethic promulgate the acquisition of knowledge and the freedom to access and disseminate information. But, as hackers contend, this information is more often managed by organizations which represent an authority structure operating counter to hacker goals. These organizations influence and are supported by a legal system that does not understand the technology and implications for basic civil liberties and property rights (Godwin, 1996). The relative influence of these organizations also extends to the mass media, which may play a role in the creation a negative image of all hackers.

Criminalization of Hacking

Portrayals of crime and deviance in the mass media influence public perceptions of crime (Cavender, 1995; Fishman, 1978; Sherizen, 1978; Warr, 1995). Direct experience of crime carries the greatest influence on opinion and perceptions of crime, but most of the populace relies on indirect information (Lotz, 1991; Sherizen, 1978; Warr, 1995). Such indirect experience is provided through media accounts of deviance and criminal behavior. The fundamental criterion in the selection of stories appropriate for the mass media is "newsworthiness" (Lotz, 1991; Sherizen, 1978). Drawing from an almost unlimited number of potential stories, gatekeepers select which stories deserve attention (Lotz, 1991; Warr, 1995). Newsworthiness reflects timeliness, prominence, novelty, or, for crime and deviance stories, the seriousness of the incident (Lotz, 1991; Warr, 1995). Thus, as Sherizen (1978) comments:

The mass media, particularly the newspapers, become sense-makers to the world, providing stocks of knowledge, available concepts (categories), and interpersonal rules (relations) by which individuals can classify and interpret crime events.

The media offer the general public a limited number of structured accounts. Use of the seriousness standard means the most spectacular occurrences are over-represented.

Reporting of crime implies that serious offenses are the most common occurrences, a claim not supported by data on criminal activity (Warr, 1995). The reporting of crime constructs a reality for the general populace (Sherizen, 1978). Reality construction plays a major role in the creation of social control mechanisms to reduce deviant activities (Cavender, 1995; Fishman, 1978; Warr, 1995).

The process of media creating images of deviance may be applied to computer crime accounts. Computer crime accounts usually focus on the spectacular occurrences. Typically, these accounts point to the public's growing dependence on computer technologies and the vulnerability associated with this dependence (BloomBecker, 1990; Kling, 1996). In these media accounts, the terms hacker and computer criminal may be used synonymously, and exaggerate the vulnerability of systems. In short, the media focus on external and even fabricated elements of the computer underground without distinguishing between motives, practices, and identities of the hackers compared with computer criminals.

A recent analysis of media portrayals of hackers indicates that most media portrayals are negative. Chandler (1996) sorts images of hackers into five categories: 1) cowboys; 2) intellectual joyriders; 3) potential murderers; 4) mentally impaired; and 5) spies. The most frequently found and more positive cowboy image includes attributes such as individualism, pragmatism, and mythic heroism (Chandler, 1996). Other images draw heavily on the threat hackers pose to the public and themselves. Elements of such negative images include the threat hackers pose to economic stability and lives based on criminal drives for thrill and excitement, addiction to computers and mental impairment, threats to sensitive systems on which peoples lives rest (i.e., air traffic control systems), and threats to the security of military or industrial information. Although some portrayals of hackers are positive, these are the exception rather than the rule (Chandler, 1996).

Negative bias in media presentations may be explained. First, extraordinary computer crime stories are financially rewarding to journalists, newspapers, and publishers. One of the most marketable products of new computer technologies is the crime story (Rosenberg, 1992). Playing on the fears of the general populace, some media portrayals reflect an attachment to outlaw cultures and individualism (Kling, 1996). Journalistic accounts portray the computer criminal as a maladjusted, sociopathic, teenage computer genius who has illegally entered a computing system for purposes of vandalism or financial gain. The inclusion of such terms as criminal, outlaw, or terrorist in these accounts makes the term hacker synonymous with illegal computer activity, and, in some instances, this usage is incorporated into laws on computer crime (e.g., Louisiana) (BloomBecker, 1988).

Second, such portrayals often are based on questionable information and a few interviews. The relationship between journalists and hackers may be one of mutual exploitation (Platt, 1997). Hackers suggest that in many instances they are aware of the journalist's drive to capture an exciting, fear inducing story, and may make exaggerated claims to see if they appear in print (Platt, 1997). In other instances, journalists are careless and do not even speak directly with individuals involved in major criminal cases (Platt, 1997). For example, the Markoff and Hafner (1995) book *Cyberpunks* provides a detailed account of Kevin Mitnick's life, the notorious "dark-side" hacker. Based on his interviews with hackers involved in the case, Platt (1997) states that the information which provided the basis for the Mitnick account was organized and manufactured, and Mitnick was not involved in the interview process. (Hafner later acknowledged that Mitnick was unfairly characterized in their account (Platt, 1997).) In addition, hackers suggest that 90% of interviews are from 20 hackers (Platt, 1997).

Third, recent research suggests that portrayals of hackers as the source of all computer crime are misleading. Those typically portrayed as computer criminals are not

computer experts or hackers, but employees and first time offenders. In a review of British studies of computer crime, Keith Hearnden (1989) concludes that 80% of crimes involving a computer were committed by employees of businesses, and that few demonstrated a high degree of technical ingenuity. More importantly, offenders were primarily first timers motivated by financial worries or drug and alcohol problems (Forester and Morrison, 1990; Hearnden, 1989). BloomBecker (1988:23) adds that computer criminals "just aren't that smart, may know next to nothing about computers, abhor challenges, and care nary a whit about the mystery of the machine." In short, the majority of those committing crime with computers do not qualify as hackers due to their lack of technical proficiency and certainly may not meet the technical proficiency level implied in computer crime accounts (BloomBecker, 1988; Forester and Morrison, 1990).

The importance of the media is apparent when considering the process of criminalizing various computing activities. Hollinger and Lance-Kadduce (1988) conclude that one of the most significant factors in the creation of legislation addressing computer crimes was the media portrayal of computer enthusiasts engaged in a wide range of criminal activities. They (1988:106) caution that during the process of criminalization the extent of computer crime is debatable, but "the number of feature articles appearing in the mass media increased dramatically through the 1970s and early 1980s." Coverage of events such as the "414 Hackers" and the motion picture *War Games* (1983) contributed to a growing perceived threat of computer crime, and helped to define computer related crimes as a major problem for the populace and legislature (Hollinger and Lance-Kadduce, 1988). The media generated a perception of threat by portraying an entire "generation of young hackers who were involved in epidemic levels of computer crime," and a poorly trained and legally powerless criminal justice system (Hollinger and Lance-Kadduce, 1988:106; Collier and Spaul, 1992).

The perceived threat stimulated industry to employ the computer security specialists and law makers to pass laws (Hollinger and Lance-Kadduce, 1988). In conjunction with experts such as Donn Parker, legislators revised laws to criminalize acts such as unauthorized computer access with the intent to defraud, malicious damage associated with unauthorized access, and trafficking in computer passwords or techniques to allow unauthorized access to systems (Hollinger and Lance-Kadduce, 1988; Johnson, 1985; Johnson and Snapper, 1985). These activities are incorporated in the revised edition of the Computer Fraud and Abuse Act of 1986, which also defined federal jurisdiction in instances of threats to national defense, governmental agencies, financial institutions, and interstate or foreign communications (Icove, Seger, and Von Storch, 1995). Most states enacted computer crime statutes which apply to equivalent state offenses.

But several cases reveal problems with laws and their enforcement. Sterling (1992), Godwin (1996), and Barlow (1996) point to instances in which law enforcement agencies infringed on the civil liberties of accused hackers or BBS operators. One case still drawing attention is that of hackers Robert Riggs, Craig Neidorf, and Rick Andrews who were a few of the many targets of a massive effort by the U.S. Secret Service termed Operation Sun Devil intended to crack down on forms of wire fraud such as credit card theft and telephone code abuse. The operation focused on the Legion of Doom, a young hacker group with no formal membership (Barlow, 1996; Sterling, 1992).

The efforts of the agencies involved in Operation Sun Devil were intensified when an alleged hacker attack on AT&T's long-distance telephone switching system occurred on January 15, 1990 (Barlow, 1996; Sterling, 1992). Although the cause of the AT&T system crash was identified as a software glitch, a series of Secret Service confiscations began. By May 9, 1990, 42 computer systems and equipment were seized along with answering machines, notes, radios, and audio cassettes (Barlow, 1996; Sterling, 1992). In

part, these confiscations were performed in search of evidence on the illegal ownership of a three page document outlining administrative procedures for the marketing, servicing, and upgrading of BellSouth's 911 operating system (Barlow, 1996; Sterling, 1992).

This document was originally downloaded from a BellSouth internal business network in 1988 by Robert Riggs. This document was uploaded to *Phrack* magazine edited by Craig Neidorf, an amateur journalist and college student, and to the Jolnet BBS, operated by Rich Andrews (Barlow, 1996; Godwin, 1996). Neidorf edited the document, and after Riggs' approval, the document appeared in the February 24, 1989 issue (Godwin, 1996). After discovering this document on his system and questioning its legality, Rich Andrews forwarded a copy of it to AT&T (Barlow, 1996). Andrews was contacted by the authorities with whom he cooperated fully. Andrews later lost his computing system in the confiscations but was never charged (Barlow, 1996). Riggs and Neidorf were arrested and indicted on seven counts including the interstate transfer of stolen property (ITSP) worth more than \$5,000 a few months following the postings (Godwin, 1996).

According to BellSouth and the indictments against Riggs and Neidorf, the 911 services document was worth \$79,499 (Sterling, 1992). Neidorf also faced fines upwards of \$122,000, 60 years in prison, and the loss of his on-line magazine along with all related computer equipment (Barlow, 1996; Sterling, 1992). Riggs' unauthorized account access into BellSouth computing systems could not be disputed, and he subsequently pled guilty to the lesser charge of conspiracy to commit wire fraud (Sterling, 1992). Neidorf pled innocent based on his First Amendment rights and the fact that he did not deprive BellSouth of property as it is defined by wire fraud and ITSP statutes (Godwin, 1996). As Godwin (1996) writes:

Under the First Amendment, the presumption is that information is free, and that it can readily be published and republished. For this reason, information gives rise to a property interest only if it passes certain legal tests. Law enforcement cannot simply assume that whenever information has been copied from a private computer system that theft has taken place.

Law enforcement officials, in Neidorf's instance (and many others), assumed that the information posted met ITSP criteria. During the trial it was discovered that the three page document was not patented, a trade secret, breach of confidence, nor could copyrighted information of this nature meet the ITSP statute; for the document could be ordered through a BellSouth catalogue for \$13 (Godwin, 1996; Sterling, 1992). Prosecutors eventually dropped charges, and a mistrial was declared (Godwin, 1996; Sterling, 1992). Although Neidorf's motion to expunge his record was granted, he was left with over \$100,000 in legal fees (Godwin, 1996).

Such cases point to the difficulty of law enforcement agencies in both understanding the technology and winning convictions. Hackers suggest that their problems result from an over-reliance on media presentations. Emmanuel Goldstein (1990), owner and editor of *2600 Magazine: The Hacker Quarterly*, states that the mass media distorted the actual events of the 911 case by suggesting that Riggs had entered and interfered with the 911 emergency system. (Riggs entered the BellSouth business system and not the telephone switching system.) The document contained no information which would provide a threat to 911 systems, and the dollar estimates for the document, reported in news accounts, were highly questionable.

Discussion on Literature

Little research addresses the nature of computer crime or hacking, and the majority of available information comes from mass media sources (Bequai, 1978; Collier and Spaul, 1992; Forester and Morrison, 1990; Hollinger, 1993; Hollinger and Lance-Kadduce, 1988; Meyer, 1989). Few direct sociological investigations exist beyond Meyer's work in 1989. Parker's investigations and conclusions were instrumental in the generation of much of the legislation enacted to regulate computer crime, but most of his data sources are the very media accounts taken for granted in other studies (Hollinger and Lance-Kadduce, 1988).

Parker's focus on the game playing mentality is consistent with the hacker's ethic. Hollinger's studies do provide insight into this aspect of computer usage, but the samples drawn from larger college populations are not representative of highly skilled computer users. In other instances, Hollinger bases his claims on samples both too small for the statistical techniques employed and not representative hackers. The more conclusive accounts of the computer underground, hackers, and the hacker's ethic are found in the work of Meyer and Denning. Yet, Meyer's accounts rely on limited interviews and secondary data sources, and Denning's accounts rely on 9 cases focused on ethical issues, not on the nature of hacking.

In all of the studies, the investigators suggest that more attention should be paid to and more research should be conducted on hackers. A social psychological perspective on hackers and hacking provides the potential to explore internal characteristics of the electronic community and hackers. Although illegal, the acts of hackers point to many important questions on the nature of information and individuals in the electronic community. These issues must be addressed given the increasing importance of computer technologies and the Internet. I address such issues by focusing on the identity of hacker as well as the role hackers suggest they play in the emerging electronic community. I also address these issues through attention to media portrayals of hackers and their reactions to them, and individual and collective aspects of the hacker identity and identity management.

CHAPTER TWO

METHODS

Studying hackers presented challenges which required the use of multiple methods. This chapter first focuses on difficulties in identifying hackers and gaining their acceptance. Next, methods used in the selection of survey respondents and electronic interviewees are presented. Then the techniques employed for the collection of both qualitative and quantitative data are discussed. Next, a discussion on the constructs used in the electronic interviews and the survey instrument are presented. Next, statistical techniques for the creation of scales and their reliability and statistical analyses used are presented. Finally, demographic characteristics of those sampled are presented

Difficulties in Gaining Acceptance from Hackers

The hacker population is not generally visible and participants in it have high levels of suspicion toward those wishing to perform investigations. My early electronic contacts were met with hesitation and suspicion on the part of hackers. On many occasions while conducting my research I was asked which federal or local law enforcement agency I represented or to verify my status as a graduate student at the University of Tennessee, Knoxville. In addition to direct requests for verification, some hackers posted my home address and phone numbers to various list-servers. Activities such as the posting of my private address and phone numbers proved serendipitous. Having my identity clearly established added to my credibility, and I believe helped me in the further recruitment of participants.

Through extended electronic and face-to-face contact with hackers and demonstrations of my own limited technical proficiency, I was able to build rapport with members of the hacking community so that I could collect data. The greatest contribution to building rapport with hackers was attendance at two conventions over the summer of

1997. The first convention was DEFCON V held in Las Vegas, Nevada between July 10 and July 13. The second convention was BEYOND HOPE held in New York, NY between August 8 and August 11. Through contact with convention organizers and convention goers, I was able to describe the project in greater detail which furthered my ability to obtain survey responses and electronic interviewees.

Sample

For this project, self-defined hackers included those individuals who identify themselves as hackers and apply the term hacking to their activities. Such individuals post home pages to the Internet identifying themselves as hackers, and provide links to other hackers' homepages. These individuals also share various forms of information through list servers, Internet Relay Chat (IRC) systems, News Groups, and conventions geared to hackers. Although many of these channels are identifiable through a search of Internet sites and discussion groups, many restrict open access to persons capable of demonstrating technical proficiency. The most accessible channels to contact hackers for this study were list-servers run by convention organizers, homepages listed by hackers, conventions, and referrals from other hackers. Thus, the population consisted of self-defined hackers who listed pages on the Internet, subscribed to the hacker list-servers run by convention organizers, attended two conventions, and were possible contacts through referrals.

Participants for this study were acquired in three ways. First, an electronic pool of respondents was selected by use of purposive, snowball sampling techniques. Homepages run by individuals or hacker organization were identified, and primary cases were identified in the following ways: by searching on-line for hacker homepages and contacting owners of these pages; by subscribing to the Dis-Org hacker list-server operated by officers of the DEFCON hacker organization; and by subscribing to the Access All Areas (AAA) hacker list-server operated by officers of the AAA hacker

organization. The initial contact included a description of the research project and me. Individual page operators were contacted directly through e-mail, and the initial announcement was posted to both list-servers. Through referrals from initial participants, others were identified and invited to participate in a similar fashion. A total of 20 initial participants were obtained through the above methods. Of those receiving questions electronically, 15 responded in the time frame to be included in analyses.

Second, cases were selected using convenience sampling at the two conventions. Conventions were selected based on recommendations from initial participants, time, and money constraints. Surveys were distributed at the first convention, DEFCON V, for the three day period of July 10 to July 13. I met with convention organizers July 9 to finalize arrangements to distribute the survey. At convention organizers request, surveys were placed on the registration table and distributed by convention workers with registration materials. I also distributed surveys from the registration table to convention goers personally, and discussed the project with them for the duration of the convention. DEFCON V surveys were either returned to a box placed at the registration table, or returned to the University of Tennessee, Knoxville Sociology Department through the U.S. mail. I made continuous checks of the box and stored completed surveys in my hotel room for the duration of the convention. A total of 457 surveys were distributed at DEFCON V, and a total of 46 were returned (43 returned at the convention; 3 returned by mail; a response rate of 10%).

In addition to the surveys distributed at DEFCON V, I also distributed surveys through a convenience sampling technique at Beyond Hackers of Planet Earth (BEYOND HOPE) in New York, NY for the three day period of August 8 to August 10. I met with convention organizers August 8 to finalize distribution arrangements, and was offered a table for survey distribution near the registration area. With the aid of a research assistant, surveys were distributed to convention goers August 9 and August 10 as they entered the

main convention area for the duration of the convention. BEYOND HOPE surveys were returned to a box on the survey distribution table, or returned by the U.S. mail to the Sociology Department at the University of Tennessee, Knoxville. Completed surveys were removed from the box at the end of each day. A total of 543 surveys were distributed to convention goers as they passed by the table, and 189 were returned (184 at the convention and 5 through mail; for a response rate of 34.8%).

Third, a list-server was established for further discussions on the research project and findings. This list-server was established for a fee of \$50 through the University of Tennessee, Knoxville computer services. The list was included in existing list-server databases so that new members could subscribe themselves. Of initial participants, 8 were signed on by me, and the remaining 16 signed on the list independently. Periodic checks of participants were made during the data collection process to ensure that those participating knew of the project, considered themselves to be hackers, and met the age restrictions set by human subjects approval. A total of 4 were dropped from the list for failing to satisfy these aforementioned criteria. The remaining 24 remained subscribed to the end of the data collection period.

Techniques

Data collection began with general content analyses of media portrayals of hackers using printed news reports, television news reports, general computer magazines, and movies. In total, 73 printed or online news reports, 28 evening television news report abstracts, and 5 movies (Appendix One) were analyzed. News reports for content analysis were selected based on Info-Track, Reader's Periodical, and Vanderbilt Television News Archive searches for the key words "hacker" and/or computer criminal. Approximately 392 articles or news reports were included in searches for these key words between 1980 and 1997. Articles which focused on other types of hackers, e.g., golfers, were eliminated from consideration. Computer magazines were used to identify specific themes related to

the computer underground which served as the foundation for both qualitative and quantitative questions. In consultation with personnel at a local video rental store, movies were selected with titles related to hacking activities or plots in which hackers play a central role in the film (e.g., War Games). The content analysis process was also used to specify media construction of hacker activities. Three research assistants content analyzed them using a coding protocol developed by the researcher over a three week period in the summer of 1997 (Appendix Two).

In addition, I subscribed to two prominent list-servers in the hacking community. The Dis-Org list-server exists as a forum for discussing techniques and motivations of hacking, as well as for sharing general information related to personal issues. This list-server is run by the organizers of the DEFCON conventions held annually in Las Vegas, NV. The Access All Areas (AAA) list-server operates similarly to Dis-Org, and includes similar forms of exchange between participants. The AAA list-server is also run by organizers of a convention held in London, England. Both list-servers report a subscribership of more than 500 each. By participating in these list-servers, I received e-mail messages, and downloaded these by topic. Over 150 text messages were included in analyses for this project. In addition, these list-servers were used to recruit respondents, and the initial call for participants was submitted to each list.

From the content analyses and participation in list-servers, open-ended questions were developed to be used as topics for electronic interaction with participants. Electronic interaction with participants began with the collection of individual level information through the use of electronic mail. Initial electronic correspondence focused on the most appropriate methods for investigation, conventions to attend, and general information on hacking. Subsequently, this procedure involved the use of qualitative questions submitted to all participants, so all answers could be compared. Hackers were presented with open-ended questions based on sensitizing concepts, and responded

through typed, text messages via e-mail. These responses were encrypted and transmitted to me through anonymous e-mail communication systems. Once responses were analyzed, follow-up questions were sent to participants. A total of 40 questions were submitted to participants included in two rounds of discussion (Appendix Three).

Following the first phase of electronic data collection, ethnographic, and survey data were collected at two conventions over the course of summer 1997. The survey instrument was constructed for both conventions, and was based on themes in media portrayals, individual on-line interviews, and existing literature on hacker activities. Questionnaires were distributed at both the DEFCON V convention in Las Vegas, NV and the HOPE conference in New York, NY. The instrument included 108 questions used to identify practices, motivations, identity, and opinions on media construction of the term hacker (Appendix Four). Ethnographic data were collected through participant observation at both conferences. Ten face-to-face unstructured interviews were conducted over the course of both conventions. In addition, general observations and impressions from the conventions, as well as presentation topics and discussion are included as data in this study.

Finally, a list-server was established to discuss the project, and to collect further information from participants. This list-server was used like an electronic focus group (Meyer, 1989; Reinhartz, 1992). General findings from the earlier phases of this investigation were presented to hackers for feedback and clarity. Most of the discussions conducted during this phase of the investigation focused on the role of hackers in the electronic community, mentoring, the hacker ethic, and media portrayals of hackers. Transcripts of discussions held on this list were downloaded and incorporated into analyses. Data were collected on this list until October of 1997 in accord with human subjects requirements.

Measures

Qualitative techniques were used to identify how hackers construct the meaning of hacker and hacking. The use of qualitative techniques such as sensitizing concepts guided question construction. A total of 40 qualitative questions were submitted to participants during this phase of the investigation. Concepts identified in the first round of qualitative questionnaires focused on respondent definitions of the terms "hacker," "hacking," and "computer underground." Comparisons were made between definitions provided by participants, and definitions were constructed for later use. In addition, qualitative questions were used to investigate the collective and individual nature of hacking, the identity and level of commitment of hackers, the processes of mentoring and becoming a hacker, and the norms and contexts applicable to hacking activities.

Quantitative techniques were used to examine constructs developed from qualitative analyses, the literature on hackers, and examination of mass media portrayals. The survey instrument consisted of 108 questions. This instrument included items focusing on elements of the hacker ethic (e.g., freedom of information, technological progress, importance of learning), mistrust of authority (e.g., law enforcement's misunderstanding of motivations and activities), definition conflation (e.g., hacker as synonymous with computer crime), motivations for hacking (e.g., personal satisfaction, freedom of information), self reported activities (e.g., unauthorized access), and the hacker and mass media relationship (e.g., images, fairness, and publicity).

Additional measures of identity, commitment, and isolation were included in the survey. Identity and commitment indicators were adapted from Callero (1987) and Hastings, Kurth, and Schloder (1996). The identity and commitment measures included questions related to the self identification as hacker, the relative importance of hacking and feelings associated with hacking, and the non-job time and money spent by hackers to engage in this activity. Anonymity measures focused on the secrecy involved in being a

hacker and the level of trust of friends met electronically. General demographic questions included in the instrument were used to collect information on age, sex, occupation, and income of respondents.

Scales and Reliability

Scales developed for this research include importance of and commitment to the hacker identity, anonymity, and motivation and self-report factors. Cronbach's alphas were calculated for each scale with a minimum value of .60 determined to be acceptable (Hastings, Kurth, and Schloder, 1996). The following discussion presents items included in each, and Cronbach's alphas for each.

The first scale, *identity importance*, was created by combining items adapted from Callero (1987) and Hastings, Kurth, and Schloder (1996). This scale includes eight questions:

Hacking is something I rarely think about.

I would feel at a loss if I were forced to give up hacking.

I really don't have clear feelings about hacking.

Being a hacker means more than just hacking.

Hacking is an important part of who I am.

Many of the people I know think of me as a hacker.

Other people I know think that hacking is important to me.

It is important to my closest friends that I continue to be a hacker.

Respondents were presented with a four point Likert response set ranging from Strongly Disagree (1) to Strongly Agree (4). Items one and three were reverse coded. Summed scores range from 8 to 32 (actual range 13 to 32), with higher scores signifying greater importance for the hacker identity in this scale that has a reliability coefficient of .75.

The second scale, *commitment*, was created from items indicating the amount of time and money spent engaging in hacker activities. The two items were:

Compared to your other non-job activities, how much of your time is spent engaged in hacking activities?

Compared to your other non-job expenses, how much money have you spent to engage in hacking activities (e.g., books, equipment, etc.)?

Respondents were presented with a four point Likert response set ranging from Not Very Much Time or Money (1) to A Great Deal of Time or Money (4). Summed scores range from 2 to 8, with higher scores signifying greater commitment to the hacker identity in this two item scale that has a reliability coefficient of .65.

The third scale, *anonymity*, included items which addressed relationships hackers have with others, the disclosure of hacker and personal identity to others, and trust of other hackers and those met electronically. This scale includes eight questions:

Only other hackers know that I am also a hacker.

I use a pseudonym online so that others will not know my real identity.

I am mostly known to other hackers by my pseudonym.

I usually don't tell people that I am a hacker.

I ask my friends not to tell people that I am a hacker.

If it comes up in conversation, I will admit to being a hacker.

I met my closest friends through e-mail or chat channels.

The people I trust most I met through e-mail or chat channels.

Respondents were presented with a four point Likert response set ranging from Strongly Disagree (1) to Strongly Agree (4). Summed scores range from 8 to 32 (actual range 9 to 32), with higher scores signifying greater anonymity in this scale that has a reliability coefficient of .71.

Responses to items which focused on motivations and the self-reported activities of respondents were factor analyzed using a maximum likelihood solution with varimax rotation and a list-wise deletion for missing values. Acceptable factor structures were identified through a minimum criterion of eigen values of one or greater as indicated by

Kim and Mueller (1978). Tables for factor analyses are included below with measures listed in order of their strength.

Table 1 presents the factor analysis results for 16 motivation items focusing on power, status, skills development, hacker ethic, thrill, and excitement. Items were adapted from the literature review, and respondents were presented statements with responses ranging in values from Very Unimportant (1) to Very Important (4). Factor analysis confirms four scales for use in statistical analyses. The first factor, *power/status*, includes 7 items related to the importance of power and control, as well as social and financial rewards as motivations for hacking ($\alpha = .71$). The second factor, *skills development*, includes 2 items related to the importance of learning and improvement of computer skills ($\alpha = .83$). The third factor, *challenge*, includes 3 items related to motivations of excitement, challenge, and fun for hacking ($\alpha = .62$). The fourth factor, *hacker ethic*, includes 4 items related to elements of the hacker's ethic such as the dissemination of information, reporting on computer problems, technological progress, and public awareness of computer issues ($\alpha = .27$). Higher summed scores on each of these measures indicates greater importance of that motivation in hacking.

Table 2 presents the factor analysis results of the self-report items along dimensions of unauthorized access, piracy, malicious damage, and theft. These self-report measures adapted from Hollinger (1993) and Elliot (1997), and focused on unauthorized access (e.g., browsing or copying files of others), deliberate damage (e.g., destroying software and hardware), piracy (e.g., copying and distributing proprietary software), and theft (e.g., stealing money or credit card numbers from other systems). Respondents were presented statements in the form of computer activities of varying degrees of severity. Respondents were asked to circle the response indicating the number of times they engaged in the activity over the previous six months. The responses choices ranged

Table 1 Communalities and Maximum Likelihood Rotated Factor Loadings for Motivation Scales of Self-Identified Hackers.

	h^2	Factor 1	Factor 2	Factor 3	Factor 4
It gives me a sense of power	.563	.850	.003	.118	-.005
It gives me a sense of control	.481	.673	-.003	.108	.145
Recognition of other hackers	.371	.529	-.005	.268	-.007
Because hacking is "Cool" or "Hip" in the eyes of other people I know	.274	.395	-.004	.003	-.237
Because I'm better at hacking than other activities	.297	.377	.184	.131	.221
To collect information on Individuals	.208	.320	.004	-.003	.006
To make money	.177	.316	-.006	-.119	.157
To improve my computer skills	.560	.002	.990	.002	.136
To learn new computer skills	.580	-.005	.668	.203	.289
For the challenge	.383	-.002	.111	.781	.004
For the thrill or excitement	.351	.104	-.002	.670	-.009
Because it is fun	.274	.149	.212	.400	.144
For technological progress	.327	.000	.228	.008	.651
To identify and report security loopholes in computer systems	.243	.000	.101	-.007	.545
To promote public awareness	.225	.004	.004	.118	.431
To disseminate information	.154	.185	.004	-.147	.297

Table 2 Communalities and Maximum Likelihood Rotated Factor Loadings for Self-Report Scales of Self-Identified Hackers.

	h^2	Factor 1	Factor 2	Factor 3	Factor 4
Copy another person's computer files without authorization	.666	.838	.010	.199	.100
"Browse" another person's computer files without authorization	.616	.795	.002	.248	.003
Make file modifications in a system without authorization	.551	.619	.176	.225	.182
Use someone's computer account without authorization	.499	.560	.129	.007	.360
Acquire another user's password	.475	.455	.155	.205	.348
Alter the source code of proprietary software	.225	.307	.208	.201	-.127
Make an unauthorized copy of proprietary software	.673	.128	.877	.006	.003
Receive an unauthorized copy of proprietary software	.710	.105	.851	.152	.194
Distribute unauthorized copies of proprietary software	.636	.150	.786	.130	.200
Deliberately "crash" a computer system	.502	.149	.158	.774	.002
Deliberately disrupt services on another computer system	.517	.214	.006	.734	.224
Deliberately sabotage another user's program	.461	.267	.008	.567	.205
Introduce viruses or worms into a computer system	.281	.230	.009	.395	.229
Take credit card numbers from another system or person	.399	.103	.173	.005	.688
Take money in electronic form from another system	.268	.005	.001	.112	.552
Take computer hardware from another person or organization	.311	.133	.123	.223	.506

from "Never Did This" (0) to "More Than Ten Times" (4).

Four activities factors are confirmed from the 16 self report items. The first factor, *unauthorized access/alteration*, includes 6 items related to the frequency of hacker activities that are defined as exploration of systems or alteration of files ($\alpha = .81$). The second factor, *piracy*, includes 3 items related to the number of times respondents engage in the copying or distribution of proprietary software ($\alpha = .89$). The third factor, *deliberate damage*, includes 4 items related to the frequency of deliberate damage to software or hardware for malicious purposes ($\alpha = .77$). The fourth factor, *theft*, includes 3 items related to the frequency with which hackers engage in theft of hardware, credit card numbers, or cash ($\alpha = .62$). Higher summed scores on each of these scales indicates a greater frequency of activity for hackers.

Statistical Analyses

As this is an exploratory project, no hypotheses are tested. Statistical techniques are used to present percentage distributions of items included in the questionnaire, and explore relationships between scales constructed. Percentage distributions are presented for all relevant items in the following chapters. The identity importance and commitment scales are used in correlation and regression analyses to indicate the strength and importance of the hacker identity in relationships with activities, commitment, and anonymity scales, as well as hackers' ages. The anonymity scale is used to indicate the degree of disclosure of information to others about their hacker identity in correlation analyses with identity importance and length of time hacking. Motivation and Activity scales are used in correlation and regression analyses with identity importance, commitment, and age. All analyses were performed using the Statistical Package for the Social Sciences.

Sample Characteristics

The sample selected for this study is comparable to prior studies of hackers (Denning, 1990; Kinross and Render, 1997). The overall response rate for the one-shot survey is 23.5% (1000 distributed with 235 returned). Of the 235 surveys returned, 182 report themselves as self-identified hackers. Survey response rates are similar to other one shot hacker surveys (Kinross and Render, 1997). The average age of respondents was 24.6 ranging from 13 to 58 years of age. The number of years of hacking experience ranged from 6 months to 30 years with an average of 8.8 years. Participants in the electronic interviews ranged in age from 18 to 55. A prior study by Kinross and Render (1997) reported an average age of 23 for respondents (range of 13 to 42) and an average number of 5.8 years of experience (n=133).

Respondents to electronic interviews were all male and white. Survey respondents were overwhelmingly male (93.3%) with 6.7% of respondents female. The majority of respondents reported their ethnicity as Caucasian/White (85.5%). The distribution of the remaining categories of Hispanic (3.5%), Asian (2.9%), and American Indian/Eskimo (1.7%) point to variation not typically included in mass media portrayals. In the final category, "Other" (6.4%) respondents created their own categories such as national status (e.g., Russian) or rejection of ethnic categories (e.g., Human Being).

Respondents also were asked to identify their highest level of education completed. The majority of respondents indicated Some College (33.1%). For the Some College response, the average number of credit hours was roughly one year at 21.58. The others in descending order were the completion of high school 28.7%, a College B.A. or B.S. 17.7%, and a Graduate/Professional degree 10.0% respectively. Grade School was reported at 3.9%. The majority of electronic interviewees reported the completion of high school, and many indicated an interest in or were attending college.

CHAPTER THREE

HACKERS AND THE MASS MEDIA

Two general perspectives on hackers emerged from the review of literature, and point to the problem hackers have with media portrayals of them. On the one hand, computer security professionals state that hackers are young (often between twelve and twenty-eight), bright (often doing poorly in school), socially inept (unable to communicate beyond the electronic realm), and with strictly intrinsic motives (addiction or thrill) (Blake, 1994; Parker, 1983). On the other hand, hackers claim that their activities are associated with intrinsic (e.g., thrill) and extrinsic motivations (freedom of information for purposes of technological progress). Further, they argue hackers are not as socially inept as computer security professionals and some media accounts suggest (Blake, 1994; Denning, 1990). Although both profiles are found in mass media presentations, more often the attributes consistent with the portrayals of hackers by computer security professionals are reported.

The problem for hackers is that the public learns about hacking through the mass media, and the majority of media portrayals negatively characterize hackers and hacking. Hackers are labeled as deviant, and societal responses are promoted to control this deviance. The computer security perspective both derives from and influences opinions of law makers/enforcers and corporate representatives on issues of data theft and destruction. The influence of computer security professionals is based on their role as experts in creating and protecting systems and information from intrusion or alteration by outsiders.

The data analysis is based on 73 text based news sources (i.e., magazines, newspapers, on-line news services) and abstracts of 28 evening television news reports from national networks from 1980 to 1997, electronic and face-to-face interviews, list-

server discussions, and 183 survey responses. The first section content analyzes mass media characterizations of hackers and hacking. Next, definitions of hackers and hacking, motivations, and activities obtained from surveys are presented. The chapter concludes with discussion of whether mass media present a distorted image of the majority of hackers, and the nature of the relationship between hackers and their computer security counterparts.

Mass Media Portrayals of Hackers

Preliminary content analysis aided construction of interview questions and differentiation of conflicting images of hackers. Content analysis produced four categories to represent the different foci of media presentations: 1) computer security; 2) computer development; 3) incident account; and 4) hacker stories. Each category is generally presented, and then the motivation and activities associated with it are described.

The computer security category includes media presentations on security measures, potential security breaches, security weaknesses, and remedies for security problems. References to hackers in these presentations often use language appropriate for describing criminal behavior, but typically with a slant invoking romantic outlaw images. Words used to describe hackers include: malevolent, unfriendly, threat, spaghetti western cool, rogue, saboteur, billy the kid, cybersnoop, malicious, and criminal. Definitions of hackers range from general negative references to "unfriendly users" and "unidentifiable visitors" to specific references to hackers as "network criminals" who break into computer systems and of hacking range from "tampering or meddling" to "a criminal activity."

Motivations and activities attributed to hackers are presented together. The motivation most frequently attributed to hackers is the desire to obtain and share information acquired through unauthorized access. Other implied motivations are desire for a sense of control or power and skill development. The activities most frequently attributed to hackers involve data theft, particularly of private information of individuals,

although Internet service providers and telephone corporations are the most frequently reported victims of hackers. The portrayals of the motivations and activities typically highlight the threat posed by hackers.

The computer development category includes media accounts about technological change or computer education. The majority of these articles are positive focusing on hackers as scientists and explorers, and emphasizing their technical skill, intelligence, and curiosity. A typical article points to the importance of hackers in the dissemination of information and the development of technology in Russia (Rogers and Bogert, 1989). Other positive ones characterize hackers as adventurers on an "electronic river" or as those who create rather than destroy. In a few instances, side references allude to hackers as "weenies," pranksters, or vandals during discussion of technological change and the fallibility of regulation.

The motivations and activities reported are consistent with the earliest conception of hackers, adept programmers or electronic explorers. Discussions of motivations highlight the importance of challenge, as well as knowledge and skill acquisition in stimulating hacker behavior. Other motivations implicitly referred to are the thrill and fun associated with it. The activities emphasized are the development of new technologies and education of others about computing. (The only reference to an activity that might be classified as negative or malicious was the introduction of the Internet Worm.)

The incident account category focuses on acts attributed to hackers and the alleged victims of those activities. These portrayals typically treat hacking as criminal in nature, but occasionally characterize it less negatively as pranksterism and vandalism. Although some descriptors might be neutral or positive (e.g., technically proficient or clever), most descriptors are negative, with some strong references to hackers as "slimeballs," "idiots," and "terrorists." Hacker activities sometimes are typified as rampages or the wreaking of havoc, and hackers as unscrupulous, irresponsible, malicious, and criminal. Definitions of

hackers range from neutral "hard core programmers" or "someone with a computer security background" to the more negative "someone who breaks into or tampers with computers." Hacking is typically defined as criminal (i.e., breaking into systems or computer trespass).

The motivations and activities match up with the computer security perspective on hacking. Motivations reported most frequently are the challenge of entering systems and the power achieved through gaining access to systems. Less frequently mentioned are boredom, thrill, theft of data, recognition of other hackers, and the "cool" nature of hacking. Activities typically are theft of data from businesses or military, forms of electronic vandalism (e.g., e-mail flood attacks and web page alterations), and threats made to individuals or groups. Descriptions of victims focus on businesses (i.e., computer companies or credit reporting agencies) and federal or state governments (i.e., military or state agencies) with a few instances of individuals.

Hacker stories, the fourth category, includes media presentations on specific hackers, their activities, and punishments. Although occasional references are made to exploration and discovery consistent with the image of the hacker as an innovative computer scientist, the majority depict hackers as technological criminals, outlaws, terrorists, and pranksters. Descriptions are frequently negative labeling hackers as disruptive criminals. Definitions of the term hacker range from negative (compulsive illegal trespasser) to very negative ("cyberthief" and "sophisticated criminals who use a computer and modem as a weapon"). Definitions for hacking are also negative with the twist that hacking as a criminal act is "more important than the goods stolen" for the hacker.

Motivations and activities in these portrayals are associated with criminal acts. Although sometimes motivations associated with the hacker ethic (i.e., challenge, technological progress, development of computer skills) are presented, more frequently

emphasized are fun, thrill, and addiction to computer usage. The activities discussed most frequently are unauthorized access to systems and unauthorized use of phone services. Some media accounts describe "social engineering" or conning persons out of information on systems and victimizing telephone companies and businesses. The victims of unauthorized access most frequently reported are military computer systems. Threats most often focused on are the theft of data such as credit card numbers and unauthorized access into vulnerable computer systems.

A few articles did not fit with these general categories, focusing on freedom of information or property rights. Most news accounts were either incident accounts or hacker stories supporting hackers' claims that the media generally portray them as deviant, if not criminal. According to news accounts, the prototypical hacker is a male who is both intelligent and obsessed with breaking into computer systems. He is motivated by the challenge of entering systems to gain access to data, which he can then steal, destroy, or use to defraud.

Based on the content analysis, many media portrayals present a blend of social types present in our society which shape public perceptions (Klapp, 1962). Three general heroic attributes appear in these portrayals: 1) *brains*; 2) *smooth operators*; and 3) *independent spirits*; with hackers typically characterized as intelligent, independent, and prone to engage in the exploitation of electronic loopholes. Also emphasized is the mystique of and shrewdness demonstrated in gaining access to corporate or governmental systems, the demonstration of power through technical proficiency. Possession of technical proficiency and an independent spirit produce the potential for a hacker's activities to run counter to rules of conduct for computer usage particularly when such rules are perceived not to be clearly established. Combined, these portrayals sketch a mixed image of hackers as clever with an intellect to be admired, but who seek power or thrill through deviant or criminal activities.

When addressing the relative threat posed by hackers, the language used in accounts varies. When accounts of theft or damage focus on individuals' computer activity and the threat of these individuals' activities is great, more villainous types are suggested such as "digital Darth Vaders," "digital Desperadoes," or "Hannibal Lectors of Hacking." Typically, such accounts point to threats or to costs incurred, as for example, recent news reports that claim computer crime costs businesses in the United States \$800 million annually, and that these costs and the number of crimes are on the rise (Fialka, 1996; Lewis, 1995). Losses often are attributed to individuals identified as hackers, and stimulate calls for specific measures to curtail the activities of hackers (i.e., increases in security measures and harsher sentencing for those engaged in such activities).

Three villainous attributes are suggested: 1) *desperado*; 2) *rebel*; and 3) *stranger*. Hackers are typed as desperadoes and rebels who are threats to an emerging electronic order which primarily serves corporations and government, and secondarily serves individuals. Their threat is specified with accounts of intrusion into governmental and corporate systems containing information vital to national, economic, or individual security. The use of analogies implying that the electronic realm is a lawless frontier supports images of the desperado. The use of language signifying a disregard for law and a technical proficiency also paints a portrait of a rebellious individual prone to disruptive behavior whether intentionally criminal or not. Also, hackers are portrayed as strangers gaining unwelcome access to systems, and as isolates whose goals are unclear and means questionable.

The majority of portrayals indicate that hackers are more villainous than heroic. This focus on deviant behaviors coupled with an emphasis on the potential criminal threat posed by hackers suggest the computer security perspective on hackers received the most attention from 1980-1997.

Hackers' Views on the Media

One set of hackers seem to see themselves as helping fortify computer security systems, and are employed or seek employment in the computer security profession. Yet, they believe hacking ultimately leads to protection of systems because security problems are uncovered. Other hackers believe that their activities are by definition criminal, and media portrayals are accurate. They may extend their activities to those considered more criminal. For most hackers, this second set of individuals are computer criminals who capture the attention of the mass media, and thus generate image problems for all hackers.

As early as the mid 1980s, hackers pointed to the negative nature of hacker depictions in the mass media (Markoff, Robinson, and Shapiro, 1985). In the early and mid 1980s, movies such as *War Games* (1983) were shown to legislators to demonstrate the potential threat hackers posed, and news reports focused on a limited number of cases of extreme behaviors heightening the perception of a threat (Hollinger and Lance-Kadduce, 1988). Such media reports often stimulated debate in the hacker community, with some hackers calling for the community to take responsibility for its activities (Markoff et al, 1985). Remedies proposed in discussions during this time were a more active role for hackers in expanding computer technologies and overt demonstrations of corporate loyalty (Markoff et al, 1985).

Hackers in electronic and face-to-face interviews, as well as on surveys frequently bemoan their negative media treatment and its repercussions. They complain the media portrayals are erroneous and falsely stereotype all hackers. From the perspective of the hacker, the media neither adequately reflect the diversity of hackers as a social category, nor do they attempt to understand this diversity. As one hacker explained in an electronic interview:

Hackers do bring up a negative image because the media have no idea what is happening and they pass these 'facts' onto everyone else. The label hacker is used for everyone in the computer underground. Even the people who go on AOL impersonating staff asking for credit card

numbers are considered hackers in the media. Many people think that being a hacker is fascinating. Unfortunately, they seem to have mental pictures of people in dark rooms with a blue glow on themselves transferring millions of dollars into their account.

As a consequence, hackers report that although they are not ashamed of being hackers, they are hesitant to identify themselves as such.

A specific difference between media portrayals and hackers' perceptions is the extreme nature of the instances reported or included as story lines in movies. Hackers reject images of obsessed "geeks" incapable of maintaining normal social relations or people engaged in criminal behavior. Although many interviewees agree that hacking can become an obsession, they argue that the extent of the obsession is far less than media portrayals imply. For example, one hacker distanced himself from the image by saying:

I dress fairly hip, I have a life, I am not obsessed with spending every waking moment on-line. I don't own any leather or rubber clothing. I don't own a pair of rollerblades. I have a fiancée', I have a tan,...[and]...I don't get beaten up because I'm a dork...[when]...The media doesn't want to come to terms with the fact that I'm 5'7" and 200 lbs, that I am capable of interacting with others,...and, most importantly, that I am just like many other hackers. We don't fit the mold they made for us so they continue to portray us the way they want us portrayed, rather than dealing with reality. Personally, when the revolution comes, I hope the media are the first ones put in front of the firing squads.

Some complain about the case of Kevin Mitnick, whose activities, charges, and convictions drew a great deal of media attention. Most interviewees say that the case is an extreme example of hacking which is not representative of the majority of hackers with one depicting Mitnick as an "animal" who "took things too far." Further, they state he deserved the punishments he received, and that his extreme obsession was the reason for his capture.

Media use of such extreme cases is important in creating drama to stimulate the interest of a public with limited understanding of computers and hackers. As one hacker sees it:

The media likes extremes, they either play us off as goofy 12 year olds with Attention Deficit Disorder and bad clothes or as hard line street criminals with laptops and hand guns. Hackers are both of those, but they're mostly something in the middle. The media doesn't want to portray hackers for what they are because, for the most part, we're boring. Imagine a movie about 'real'

hackers. Who in their right mind would want to spend \$7.00 to see me sitting in front of a computer in my underwear, cursing and smoking for 2 hours?

Another hacker puts it this way:

Hacking is quite dull to the ordinary person. The media hypes it up and portrays hackers as twisted teenagers with malicious agendas. In movies they portray it as a graphical fantasy with spectacular color and exciting action. A hacker may spend thirty hours pasted to a computer monitor watching repetitive text scroll across his/her screen. The media is far off.

Respondents believe explanations of hacking would be soporific rather than dramatic, for as one participant indicates, "If I were to explain to you the details of a simple attack (like an ip spoof going for the .rhosts or root) I could put you to sleep in about 5 minutes."

Respondents claim public perceptions of threat reflect media misrepresentation or as one participant simply states "They [*the general public*] follow the media."

Television news reports are seen as particularly problematic because of their limited depth due to television time schedules. One hacker focuses on the problems of doing a television interview:

I hate TV news, because if they can't get a camera there, it probably didn't happen. Also, they can interview for hours, ask all the right questions, respond well to the hacker giving the impression that the interview will be positive, and then get it back to the editing suite, and chop the heck out of it!!

This hacker further states that:

[*as an interviewee you*] Always have quick sound bites ready as answers to the most basic questions. You're NOT talking to the talent who's got the microphone in your face. You're not even talking to the camera man or the sound guy. You need good sound bites that the video editor back at "The Shop" will think are SO good, that s/he MUST use them in the story.

Other hackers suggest that bias exists and specific networks are particularly negative and the special programs and the interviews they present are "lame."

The survey data show similar belief patterns about conflation, exaggeration, and contrived creation in media accounts. Hackers generally believe that their media image is negative, their influence over the public and law makers' opinions of them is limited, and their public image problems are due to the media. Table 3 presents the distribution of responses to questions on fairness, conflation of computer crime and hacking, and the

Table 3 Percentage Distributions for Statements Regarding the Fairness of Printed and Television News Reports.

	Strongly Agree	Agree	Disagree	Strongly Disagree	N
Printed News Reports:					
Present hacking in a fair manner	2.2	4.9	45.4	47.5	183
Confuse computer crime with hacking	48.1	45.4	4.4	2.2	183
Contribute to a negative image of all hackers	48.4	44.5	3.8	3.3	182
Television News Reports:					
Present hacking in a fair manner	2.2	3.3	49.7	44.8	183
Confuse computer crime with hacking	50.8	42.6	4.4	2.2	183
Contribute to a negative image of all hackers	51.9	39.9	5.5	2.7	183

(Percentages may not equal 100 due to rounding)

contributions of media accounts to a negative image. Respondents generally disagree with statements asserting the fairness of hacker portrayals in both printed and television news accounts. Further, they generally agree that both printed and television news accounts confuse computer crime with hacking and contribute to a negative image of all hackers.

Table 4 presents perceptions of the relative influence of media sources on the law makers and the general public. The majority of respondents believe that both printed and television news reports have moderately high to a great deal of influence on law makers' perceptions of hackers. A similar pattern of belief appears about printed and television news reports exercising strong influence on the general public. When asked the extent to which information from hackers may influence law makers' or the public's perceptions of hackers, the majority indicate that the information hackers provide has a moderate influence or no influence.

Some hackers do play a role in media exaggerations. Negative images in media quotes of hackers emphasize hackers' skills, the vulnerability of computer systems, and threats to systems or corporations. Pointing to their skill, some members of the hacker group Masters of Deception were quoted from Secret Service wire taps as stating "We can destroy people's lives or make them look like saints" (Quittner, 1995). Other quotes from interviews focus on the availability of information and the lack of security which provide the basis for breaching computer systems. For example, hackers say they can acquire such information as credit card numbers or system operations easily through the trash, and are not challenged by "dumb" persons working in corporations (Schiffres, 1985).

Some image problems result from actions. Media accounts may report on hackers' alteration of web pages including the insertion of obscene material and threatening statements. One hacker group using the name H4G1S (Hagis written in a form of computer slang) threatened on the altered NASA page that "During the next month, we

Table 4 Percentage Distributions for Perceived Influence of Media Sources and Hacker Sources on Law Maker's and the General Public's Perceptions.

	Great Deal of Influence	Moderately High Influence	Moderate Influence	Moderately Low Influence	No Influence	N
Influence on Law Makers:						
Printed News Reports	37.0	37.0	18.2	5.5	2.2	181
TV News Reports	44.2	32.6	16.0	5.0	2.2	181
Information from Hackers	8.8	5.5	12.7	35.4	37.6	181
Influence on General Public:						
Printed News Reports	30.2	34.1	29.7	4.4	1.6	182
TV News Reports	57.7	25.3	10.4	4.4	2.2	182
Information from Hackers	8.2	10.4	18.1	44.0	19.2	182

(Percentages may not equal 100 due to rounding)

the members of H4G1S will be launching an attack on corporate America." The Department of Justice and the Central Intelligence Agency pages were reported to have experienced similar alterations. A few hackers have gone so far as to repeatedly physically threaten a reporter. For example, news reporter Richard Sandza was electronically tried and convicted by hackers for an article he wrote in *Newsweek* magazine. Sandza was harassed over the telephone by hackers with threats ranging from exile to death, "We're going to disconnect your phone...We're going to blow up your house"(Sandza, 1984:81).

Hackers' Perceptions of Hackers and Hacking

Definitions of Hackers and Hacking

Definitions for hacker and hacking offered by participants in electronic and face-to-face interviews point to hackers as individuals with a high interest in learning and self direction. One interviewee defines a hacker as, "somebody that likes to learn, someone with a high learning curve, someone who likes to push the limits." Many interviewees argue that this interest in learning requires a hands on approach, a great deal of patience, and self direction. Others propose all hackers are generally concerned with learning the operation of any system. Integral to these descriptions are references to performing tasks in clever or "non-standard" ways as a way to learn. Almost all participants emphasize that hacking requires self-direction because it involves long hours of reading technical manuals and programming. As one hacker succinctly said, "You don't get taught, you teach yourself."

Respondents distinguish between simple programming and more detailed operations when referring to the hands on nature of hacking. One clarified, "Hacking is not running a script from your Windows 95 machine to automatically fish for credit card numbers or username/password pairs on AOL [*America On-Line*], just like it is not hacking to crash computers with ready-made programs." Some participants point to the importance of learning, having patience, and using a hands on approach as characteristics

which may qualify hackers as explorers, freedom fighters, or pioneers of the electronic realm.

One common distinction in hackers' definitions is the difference between hackers and computer criminals. According to most interviewees, hackers do not steal or destroy; they are "merely exploring areas that they are interested in." True hackers do not steal or "cause damage to data, computers, companies, or people." Those making these distinctions state that hacking is nothing more than the pursuit of knowledge, and that extreme cases reported in media sources exaggerate their activities and conflate them with computer crime. Thus, a true hacker "is someone who wants to learn, not extort."

A minority do not so clearly distinguish hackers and computer criminals. Some suggest that by definition some hacking activities are criminal focusing on laws which criminalize them. Criminalization of unauthorized access is at the core of the assertion of hackers who state "in your world we are [*criminals*] but in ours we are not." One hacker distinguishes:

There are computer criminals that are hackers but not all computer criminals are hackers; just like not all hackers are computer criminals. For hacking to be considered a crime, at least to hackers, there is a line. Nobody is quite sure what that line is. Personally, along with others, I think it is something like an obvious physical or otherwise damage to the system. This means like deleting files, but not copying files, like the E911 problem.

Echoing these distinctions, another hacker states:

Some are, some aren't. Not all hackers break the law. Those that do are criminals. The law may not be a just one, but that doesn't mean that you're not breaking it. In the past I would have argued that you had to break into computers to learn. Today that isn't really true. To get on the Internet I had no real choice. It was either break into a college, or not get on. But those times have changed. For less than twenty dollars a month you can live on the Internet, and if you want to run Unix, shell out a few hundred dollars for an old PC.

One hacker states that breaking into systems is at the core of what it means to be a hacker.

This hacker complains that:

It makes me sick how hackers attempt to justify their actions or how the underground in general has broadened the scope of the word 'hacker' to include people who have never broken a system,

piece of software, or piece of hardware before in their life...any hacker who can't deal with...*[the criminal nature of their activities]*...and tries to justify their actions shouldn't be hacking.

Essentially, these individuals point to one area of controversy found in the hacking community, the lack of a distinct line between hackers and computer criminals.

Experiences and Beliefs

Although definitions of the term hacker vary, participants share many experiences and beliefs. For instance, most participants classified themselves as intelligent but unchallenged in school. One hacker says, "I was always ahead of my class and felt like they were slowing me down. Even in 'AP' classes, I continually felt like I could move faster." In a similar fashion, another hacker explains:

I used to finish all my homework for the day in my classes while the teacher taught. I would fall asleep in class and be woken up by the teacher and asked the answer to a question, which I would then answer correctly and go back to sleep. They eventually left me alone. The fact that I got horrible grades resulted from the fact that school didn't challenge me, so I never paid much attention.

Despite the lack of interest in school, many electronic interviewees report attending college or completing college degrees and working in the computer industry with prestigious firms either while in school or currently.

The beliefs of hackers on freedom of information and technological progress are similar. Many contend that information should be free, and that free information is at the core of both technological progress and their hacking activities. Participants distinguish among types of information. Specifically, public information which should be accessible is distinguished from proprietary or potentially dangerous information which should be protected. As one hacker explains:

I believe in the freedom of most information. If you find someone that says 'freedom of all information', then ask them for their social security number and their credit card numbers. It just can't work that way. As far as hacking information, I believe in information for the masses to a certain degree. If there is a new exploit out that requires a decent level of understanding to use it, then it shouldn't be given to just anyone, especially if it is 'automated.' The idea of hacking is to learn what's out there, and learn the system, not to give clueless newbies *[neophyte hackers]* an arsenal that lets them break into any system.

Another hacker puts it this way:

Freedom of information? I don't follow the hacker bullshit of 'information wants to be free'. It's just a pathetic attempt to justify what they do. Information should be publicly available but it shouldn't all be free. I don't hack to liberate information.

Others specify that the only instances in which private information should be made public are those which make clear flaws in computer system security. Some list server discussions debate the importance of respecting the economic nature of information with some participants arguing that rising software prices justify piracy because they are too expensive.

In all electronic and face-to-face interviews, participants stressed the importance of technological innovation. Many argue that access to information and reporting of such security flaws reflect the role that hacking may play in promoting technological progress. Others point directly to hacking as a possible causal factor in the evolution of computer technologies. One respondent states that:

If it wasn't for hacking, nothing new would ever get invented. I like to feel that I am a part of something and that I'm doing something that is via one means or another going to change things (i.e., making networks more secure, making software more stable). We're the ones that kick the tires to make sure things don't fall apart.

In some instances, list server discussions emphasize the importance of technological development and the role that regulations may play in preventing it. In these contexts, hackers often emphasize the risks involved in breaking both unauthorized access and theft laws.

They express opinions on the degree to which law enforcement agencies are interested in their activities and the relative effectiveness of laws criminalizing hacking activities. Some hackers suggest that laws do not address the potential to penetrate computer systems and computer penetration laws are inherently unenforceable. As one hacker claims:

They are afraid of our capabilities. We are not afraid of our capabilities. WE know that any system can be cracked. Laws? This is the businessman's solution to a technical problem. Technological problems require technological answers, not unenforceable laws.

With the use of similar logic, other hackers claim that the law enforcement community is not interested in the majority of hackers; its only interest is in the few posing a threat. One participant offers:

I don't think 90% of law enforcement gives a fuck about 90% of the hacker community. The hacker community has become so fucking stupid in the last 5 or 6 years to the point that 90% aren't a threat to anyone other than themselves. Current laws are vaguely written and randomly enforced...according to the current law, you are breaking the law right now by owning a telephone and a computer because they could be tools of fraud. I don't think the laws reduce much of anything...

Many hackers suggest that law enforcement officials "cracking down" on them are ignorant of technology and therefore unable to distinguish real threats from perceived ones.

Survey responses substantiate the positions taken by hackers interviewed on technological progress, lack of understanding, and the ineffectiveness of laws (Table 5). The majority of respondents agree that the laws regulating electronic behavior in general and on the Internet are unnecessary and the result of overreaction to mass media presentations. The majority also either agree or strongly agree that violation of laws is necessary for technological progress, and that property rights slow the rate of technological change. A substantial minority disagree or disagree strongly with both statements. This dissent may reflect differences between those hackers adopting a computer security perspective on system protection and those adopting a freedom of information perspective. Whatever their views about the laws, the majority disagree or strongly disagree with computer crime laws discourage hacking, and agree or strongly agree that law enforcement agencies fail to understand the motivations and activities of hackers.

Table 5 Percentage Distributions for Statements on Computer Crime Laws and Lack of Understanding of Law Enforcement.

	Strongly Agree	Agree	Disagree	Strongly Disagree	N
Computer Crime laws are an over reaction to media presentations	44.0	40.1	14.3	1.6	182
Violating computer crime laws is necessary to improve computer technologies	23.3	41.1	30.0	5.6	180
Property rights slow the rate of technological change	19.2	46.9	26.6	7.3	177
Computer crime laws discourage hacking	9.4	23.2	33.1	34.3	181
Law enforcement agencies do not understand the activities of hackers	56.0	35.2	7.7	1.1	182
Law enforcement agencies do not understand the motivations of hackers	65.9	25.8	6.0	2.2	181
Laws are not necessary to regulate behavior on the Internet	29.5	38.8	25.7	6.0	181

(Percentages may not equal 100 due to rounding)

Motivations

Many hackers take the position that knowing their motivations is the key to understanding their activities. For them, desire to learn and experience challenge motivates their activities. Some refer to hacking as an intellectually thrilling and fulfilling game. This game is played interactively with computers to accomplish the task of "making the machine do what I want it to do" or to acquire a "sense of being somewhere that could possibly be off limits to me." The rewards of this game are a sense of power or a "rush."

As one hacker brags:

Hacking is all about power. Teens have little power in the world around them, but it is a time when that is changing for them. Young girls manipulate boys. Young boys manipulate things. Cars or computers, it's all the same. Boys manipulate objects to control the world around them, while women control people. So I took to the computer, I made a name for myself. I controlled the world around me.

Another hacker describes it as an ego builder:

Hacking is a huge rush, and probably also an egotistical thing for me. The main thing is the rush, though. I can feel that I, a single person in my room on a 14.4 modem and a laptop, have beaten the huge faceless company hundreds of miles away in a game...The egotistical part is where I can look around my school and see people who I think will not pass the 11th grade, drop out and become bums, and then I look at myself and think how I'm already playing with the big boys who make lots of money.

Motivations mentioned less frequently were making money and impressing other hackers.

Two points must be made about impressing other hackers. First, participants claim that impressing others is far more important when one is a novice hacker. As one gains recognition as a hacker, hacking becomes a self directed activity geared toward learning and challenge. Early in one's hacking career it is important to impress others by breaking into systems and bragging about it. Such bragging is an early "phase" in a hacking career.

As a hacker states:

I've been doing this for 12-13 years now, and I am so over that stage. I honestly don't give a rats ass about what anyone thinks about me, maybe that why I'm respected, because I'm doing it for myself and not for anyone else now.

Second, recognition from other hackers is no longer important because of the level of expertise necessary to enter the hacking community has changed. Pointing to the lack of skill of some persons identifying themselves as hackers, one participant states:

Very few people's opinion bothers me. I could care less about acceptance in the hacking community. Today most in the scene are a bunch of idiots that use windows and can't program at all. asking for warez [*pirated software, some forms of which may be used to crack systems*] and calling themselves hackers.

Hacking simply becomes an end in itself.

Survey data collected at both conventions corroborate the importance of these motivations (Table 6). The majority of respondents identified motivations such as challenge, thrill, learning (new or improving computer skills), fun, and self fulfillment as important or very important to their hacking activities. Similar patterns may be identified from fun/thrill and skill motivation scales (challenge, $\bar{X} = 9.6$; skill, $\bar{X} = 7.2$). Two motivations, sense of power ($\bar{X} = 4.16$) and control, are rated as unimportant or very unimportant by the majority not supporting interview data. Motivations such as the recognition of others and the "hip" nature of hacking are rated as unimportant or very unimportant by respondents. Perceptions of motivations regarding appropriating information parallel those hackers expressed in interviews, i.e., collecting and sharing information on computer systems is considered more important than collecting and sharing private information on individuals.

Activities

Survey responses on selected hacking activities (unauthorized access/alteration, theft, deliberate damage, and software piracy) confirm interview data on hacker definitions of activities. Unauthorized access activities are the ones most often referred to by hackers in face-to-face encounters and found in news sources (Table 7). The majority of respondents report engaging in each of these activities six times or less over the six month period prior to completing the survey. In addition, roughly 20% or

Table 6 Percentage Distributions for Importance of Motivations in Hacking Activities.

	Very Important	Important	Unimportant	Very Unimportant	N
For the challenge	46.7	46.7	4.9	1.6	182
For the thrill or excitement	25.8	46.7	20.3	7.1	182
To learn new computer skills	70.9	27.5	.5	1.1	182
It gives me a sense of power	4.4	23.6	44.5	27.5	182
Recognition of other hackers	2.2	14.8	44.0	39.0	182
Because it is fun	44.8	50.3	3.9	1.1	181
Because I'm better at hacking than other activities	11.0	21.4	42.9	24.7	182
To improve my computer skills	64.3	32.4	2.2	1.1	182
Because hacking is "Cool" or "Hip" in the eyes of other people I know	-----	2.2	37.6	60.2	181
To collect information on Individuals	4.4	24.4	38.3	32.8	180
To collect information on computer systems	30.7	54.7	9.5	5.0	180
It gives me a sense of control	5.5	25.4	43.6	25.4	181
To identify and report security loopholes in computer systems	24.3	45.9	20.4	9.4	181
To disseminate information	31.6	39.5	19.8	9.0	178
For technological progress	36.5	49.2	9.4	5.0	181
To make money	5.6	15.0	28.9	50.6	180
To promote public awareness	17.9	29.6	31.8	20.7	179
For Self Fulfillment	28.5	52.5	13.4	5.6	179

(Percentages may not equal 100 due to rounding)

Table 7 Percentage Distributions for Unauthorized Access/Alteration Activities Over the Six Month Period Prior to Completing the Survey.

	Never Did This	1 to 3 Times	4 to 6 Times	7 to 10 Times	More than 10 Times	N
Acquire another user's password	13.6	25.6	19.3	9.1	32.4	176
Use someone's computer account without authorization	19.2	23.2	13.6	7.3	36.7	177
"Browse" another person's computer files without authorization	11.9	28.4	18.2	7.4	34.1	176
Copy another person's computer files without authorization	21.5	36.2	11.3	6.2	24.9	177
Make file modifications in a system without authorization	31.6	35.0	10.2	4.0	19.2	177
Alter the source code of proprietary software	51.1	27.5	10.7	3.9	6.7	178

(Percentages may not equal 100 due to rounding)

more indicate "more than 10" times for the first four activities related to unauthorized access/alteration. The distribution of responses is bimodal; 1 to 3 and more than 10 are modes for all but one activity.

Table 8 presents the distribution of self reported activities related to theft over the six months preceding completion of the survey. The clear majority of respondents report never engaging in any of the activities during the six month period. Of those who engaged in these activities, typically the frequency of activity was quite low. This finding is contradictory to media portrayals. In face-to-face interviews hackers stated that if they engage in theft, it is typically in the role of computer security specialist testing computer systems, rather than as gain seekers.

Table 8 Percentage Distributions for Electronic Theft Activities Over the Six Month Period Prior to Completing the Survey.

	Never Did This	1 to 3 Times	4 to 6 Times	7 to 10 Times	More than 10 Times	N
Take computer hardware from another person or organization	63.1	23.5	6.7	1.7	5.0	179
Take credit card numbers from another system or person	74.7	10.7	5.1	2.2	7.3	178
Take money in electronic form from another system	92.7	2.8	2.8	---	1.7	177

(Percentages may not equal 100 due to rounding)

Table 9 presents the frequency of engaging in activities involving deliberate damage for the previous six month period. For each behavior, the majority of respondents report never engaging in the activity for the six month. Of those respondents who did engage in the activities, the most frequent level of activity was one to three times.

Table 10 presents the distribution of self reported activities related to software piracy for the same time period. For each behavior, the majority of respondents report never engaging in it for the six month period. Of those who did engage in the activity, the

Table 9 Percentage Distribution for Deliberate Damage Activities Over the Six Month Period Prior to Completing the Survey.

	Never Did This	1 to 3 Times	4 to 6 Times	7 to 10 Times	More than 10 Times	N
Deliberately damage computer hardware	93.8	3.4	1.1	.6	1.1	178
Deliberately damage computer software	87.1	6.7	2.2	.6	3.4	178
Deliberately "crash" a computer system	63.6	22.7	5.7	1.7	6.3	176
Deliberately disrupt services on another computer system	58.7	25.7	6.1	2.2	7.3	179
Deliberately sabotage another user's programs	79.7	14.7	1.1	1.7	2.8	177
Introduce viruses or worms into a computer system	81.6	10.6	3.4	.6	3.9	179

(Percentages may not equal 100 due to rounding)

Table 10 Percentage Distribution for Software Piracy Activities Over the Six Month Period Prior to Completing the Survey.

	Never Did This	1 to 3 Times	4 to 6 Times	7 to 10 Times	More than 10 Times	N
Receive an unauthorized copy of proprietary software	92.7	2.8	2.8	—	1.7	178
Make an unauthorized copy of proprietary software	74.7	10.7	5.1	2.2	7.3	178
Distribute unauthorized copies of proprietary software	63.1	23.5	6.7	1.7	5.0	177

(Percentages may not equal 100 due to rounding)

most frequent response was one to three times. Illegal software distribution generally is considered an activity requiring a lower level of computer skill and this may be one reason for the low percentages reporting such activities.

Some hackers engage in deliberate damage or theft, so the question becomes to what extent are unauthorized access activities associated with deliberate damage or theft. With the use of self-reported activities scales discussed in chapter 2, Table 11 presents correlations between self-reported activities for participants. Significant and moderately strong correlations exist between each of the self-reported activities scales. Similarly, the relationship between unauthorized access/alteration and theft indicates that the more one engages in unauthorized access or alteration of electronic information the more likely one is to engage in electronic theft. The relationship between unauthorized access/alteration and deliberate damage indicates the more one engages in unauthorized access or alteration of electronic information the more likely one is to engage in deliberate damage to systems or hardware. Interviews suggest that hackers would argue these relationships indicate that many may engage in unauthorized access but few actually engage in theft or destructive behavior. Further, many hackers argue that those individuals most likely to engage in theft or deliberate destruction or theft are also likely to engage in unauthorized access, but engaging in unauthorized access does not necessarily indicate destruction or theft of data.

Table 11 Pearson Product Moment Correlation Coefficients Matrix of Self-Reported Activities Scales.

	Unauthorized Access/Alteration	Piracy	Theft	Deliberate Damage
Unauthorized Access/Alteration	1.00			
Piracy	.345**	1.00		
Theft	.299**	.282**	1.00	
Deliberate Damage	.515**	.306**	.364**	1.00

*p<.05; **p<.01

Exaggerations and Media Accounts

These self reported activities and relationships support some media claims on the activities of hackers. Most hackers interviewed acknowledge that they are in part responsible for their negative image. But they suggest that hackers or more often "wannabee" hackers may exaggerate their activities to reporters with the hope of gaining recognition and status in the hacking community. One hacker comments on bragging behavior:

In fact, some well known hackers do that *[exaggerate their claims]* regularly *[which]* makes me sad. They can bullshit all they want about things they haven't done, because they can't get into trouble, but they don't realize that the media will use it against the entire community...*[these]*...hackers regularly exaggerate their activities to the media in hopes of making themselves look cool and hoping to gain respect from their peers. If that's why you're hacking, then do us all a favor and go find another hobby.

Others propose that reporters do not verify the authenticity of interview sources allowing individuals inappropriately identifying themselves as hackers to foster the negative image of all hackers. As one hacker complains:

Reporters make no effort to ensure they are talking to a real hacker when they do an interview. They will often end up talking to some 14 year old that has seen the movie "Hackers", deleted his teacher's machine, then calls himself a hacker.

Whether the blame is partially placed on reporters for not verifying their sources as authentic hackers or on "wannabees" creating hacker stories, hackers agree that exaggeration of their activities occurs and contributes to a negative public image.

Survey data also support the argument that some hackers may play a role in the creation of a negative image for all hackers (Table 12). When asked in person, many hackers express concern about their public image, and hacking conventions have panel discussions on the media treatment of hackers. But, in this survey the majority disagree or strongly disagree with the statement "In general, hackers are concerned with their public image." Statements about publicity seeking or media manipulation by hackers elicited stronger negative responses. Respondents split fairly evenly over hackers' willingness to

make exaggerated claims. The discrepancy between electronic/face-to-face interview responses and survey responses may reflect the wording of the questions (i.e., reference to all hackers which in many instances would not be true) or social desirability (i.e., bravado or support for claims of media exaggeration found in the hacking community), as well as sample differences.

Table 12 Percentage Distributions for Hackers' Perceived Publicity Seeking and Exaggerated Claims Making Behavior.

	Strongly Agree	Agree	Disagree	Strongly Disagree	N
In general, hackers are concerned with their public image.	5.5	35.2	46.7	12.6	182
Hackers strive for publicity	2.7	25.7	50.8	20.8	183
Hackers attempt to exploit reporters for personal recognition	2.8	23.8	43.6	29.8	181
Hackers will exaggerate their activities to reporters to see if they are printed	12.2	33.7	33.7	20.4	181

(Percentages may not equal 100 due to rounding)

Discussion

The media treatments content analyzed incorporate elements of both heroic and villainous categories for hackers. Heroic attributes in these media treatments include references to the intelligence and independent spirit of hackers. Central to the positive nature of these attributes is the incorporation of a technical proficiency, creativity, and willingness to reject convention to accomplish some task (Klapp, 1962). Villainous attributes include references to hackers as threats to an emerging electronic order and intruders to systems. Central to the negative nature of these attributes is the incorporation

of images of a lawless, rebellious, and intrusive character (Klapp, 1962). Variation in the use of language indicates that the relative threat portrayed in the mass media is a significant factor in assigning hackers to a general social type. Instances of media treatment that point to hackers as a great threat are more common, and draw more heavily on villainous attributes. These villainous characterizations are more consistent with a computer security perspective on hackers, and indicate that hackers' concern over their media image may hold merit.

The mass media present the discrepancy between the rules of conduct for computer use expressed by computer security professionals and hackers. Focusing on activities such as unauthorized access as a form of illegal computer use, computer security professionals specify that these activities are consistent with the behavior of those identifying themselves as hackers. According to these specialists, such activities pose a threat to information that these computer security professionals are employed in protecting. Based on their occupation, the power of computer security specialists is derived from their relationship to law makers and corporations. This relationship provides computer security experts the power to define acts as deviant which is greater than the power of hackers to avoid deviant labels. This power difference coupled with a vested interest in portraying hackers as a threat, ensuring continued employment, encourages computer security professionals to frame debates over computer security.

The majority of media portrayals analyzed point to hackers as a threat to personal, corporate, and governmental information. Elements of these portrayals include references to hackers as meddlers engaged in a criminal activity motivated by power, control, or challenge. Electronic interviews and survey results indicate such characterizations which often draw on exceptional cases which do not reflect the behavior of the majority of the loosely constructed community of hackers. Although many activities may provide a thrill or rush for some, hackers indicate that these activities are guided by a more general

motivations; those being, knowledge or skill development, rather than the intent of theft. In addition, many hackers interviewed uniformly support the importance of security in protecting certain forms of information, and express an interest in working in the very industry that actively labels them as deviant; what may be viewed as an incestuous relationship.

The differences between media portrayals and the self reported activities and motivations of hackers are crucial. Computer security professionals try to define and guide policies based on the argument that hackers pose a threat to computer systems and the information held in them. Hackers engage in activities perceived to be deviant by the computer security professionals. Such a division is common to public debates over the nature of collective deviance, and such debates often focus on allegations of illicit behavior by one group using another as the target (Becker, 1963). Given that many hackers eventually engage in computer security work, this relationship may indicate that there is an interesting twist in the labeling process of hackers; that being, that persons labeled as deviant are ultimately the ones who wish to protect systems professionally.

Hackers are aware of how they are perceived by computer security professionals through contacts at hacker conventions and the mass media. This reflexivity affords certain members of the hacking community the opportunity to contribute to a negative image that they believe is consistent with their own definitions of hacker, and ultimately this contribution to a negative image is where the diversity in the hacking community becomes apparent. Some hackers interviewed indicated that hacking by its very nature is a criminal enterprise. For these individuals, claims on the unfair media treatment of hackers are nothing more than justifications for activities which break the law. On the other side, some hackers suggest that such individuals are not hackers, but computer criminals. The vocal deviants proclaiming their clever crimes may play a central role in creating a

negative image of all hackers in that they serve as exemplars for all hackers in media accounts.

The statements of some hackers about the criminal nature of hacking may, in part, be accurate. Although the generally shared goals of hackers may be learning and developing skills, they do engage in activities that have been criminalized. Activities such as seeking unauthorized access combined with intrinsic motivations such as challenge and thrill portray individuals who may be less concerned with the legality of their activities than the activities themselves. Motivations such as freedom of information or technological progress are often presented by participants in the context of rationalizing a behavior which stems from intrinsic motivations such as challenge and thrill. Such activities and motivations draw the attention of the mass media and law enforcement, and also serve as examples for computer security professionals as activities which are both intrusive and costly. There may be different types of hackers; some for whom the deviant label is more appropriate for others. Differences of opinion on the nature of hackers stem from a discrepancy in opinions on the identity of hacker not reflected in media portrayals and indicate that more traditional hackers may have lost control of the meaning of the hacker image.

CHAPTER FOUR

THE HACKER IDENTITY

Becoming identified as a hacker results from passing through various career phases. In this chapter data are presented to describe those career phases. The first section discusses the early experiences of novices and influences important to adopting the hacker identity. Next, the relative importance of and commitment to the identity are presented. The final sections point to problems hackers experience in maintaining control of the meaning of the hacker identity.

Identity Development and Interaction

Models of deviant careers outline the process of acquiring and becoming increasingly attached to a deviant identity, such as hacker (Becker, 1963). A deviant career begins with a perceived nonconforming act and may proceed to embracement of a deviant identity and a preference for association with others sharing the deviant identity (Becker, 1963; Rubington and Weinberg, 1973). Models of deviant careers tend to emphasize a passive person who is acted on by social forces, although Rubington and Weinberg (1973) and others acknowledge that some individuals may more actively pursue deviant identities and careers. Hackers actively seek out others sharing their interests early in their deviant careers and continue contacts with similar others throughout the development of their hacker identity. Models of deviant careers such as Becker's were used to create a template for active pursuit of the hacker identity.

Typically, the career of the hacker begins in adolescence with a general interest in technology, a desire for learning, a search for stimulation, and a need to explore. As one hacker explains, "it just seems that I like anything that challenges my mind and is invigorating, computers included." For interviewees this interest began with their introduction to computers between the ages of 8 to 18 (the mean age for survey

respondents is 15.4). Many participants indicate that their earliest experiences with computers were at school or through friends, with some willingly bartering their labor for access to systems. One experienced hacker recalls:

I hung around the computer room getting paper clips and erasers and other supplies for the lady running the room until she kicked IBM in the rump enough times to get a Programmed Instruction Book set on Fortran. I took one book home, came back and swapped it for the next book in the series, and started punching cards shortly thereafter.

All hackers perceive that their first experiences with computers played an important role in shaping their current activities.

Most interviewees believe that it was the ability to electronically or face-to-face communicate with others like themselves which marked the formal beginning of their hacking activities. Nonconformity to standards of computer usage (hacking) is rooted in early experiences such as the trade and distribution of pirated software. A hacker remembers:

When I was 10 my parents got an 8088 XT computer. Previously I had gotten a taste of having a computer and a modem from using a borrowed Commodore 64 and 300 baud acoustic coupler modem. I swapped C-64 warez [*Commodore 64 software*] until I got my IBM. My parents didn't want to get me a modem for the IBM cuz they were afraid of hackers/virii. The MIS director at their work convinced them that a modem was totally harmless and they should get it for me. They finally got me a 2400 bps modem. The MIS director ran a bulletin board at the company and let me on it. Turns out he was a software pirate so I started swapping warez with him. Slowly I began to make my way onto other warez boards and was soon trading all over my area.

Most of the interviewees describe similar experiences, and state that contact with others exploring systems provided the stimulus for further activities.

Increased electronic interaction with people playing with computer systems appeared to encourage interviewees to increase their level and frequency of deviant activities. Budding hackers draw on three principal sources: mentors, peers, and mass media. The hacker mentor/neophyte relationship focuses on the importance of demonstrating self direction and technical competence. The typical mentor supplies a list of books and directs the neophyte to resources on the Internet, but rarely takes the time to

offer information beyond answering questions. One hacker recounts his experiences with a mentor:

It started when I met someone on a BBS who showed me some tricks on the board that were definitely not normal. When I asked him how he did it, he told me about a book he had read and figured the tricks out on his own. He told me the name of the book, I went out and bought it, and figured out how he did it. I was so excited (I guess that would be the word for it) that I had figured out on my own that I started buying books and programs nonstop and played with them until I had figured out the secrets that all programs have (like security holes).

One hacker mentor explains:

I'm a busy guy. I work long hours, I have a life, I have a fiance', and I really don't have the time to go hang with someone half my age and teach them to hack. I'll answer questions but that's about it. I'd point them in the right directions of where to go get info.

The burden of proving self direction and technical competence is on the neophyte hacker who must comprehend the initial materials before the mentor takes a more active role in the education of the neophyte.

Technical expertise is demonstrated in two ways: asking technically complicated questions of peers or announcing a form of electronic coup counting. Most interviewees believe the technically complicated question is the best indicator of a hacker. If a question demonstrates a technical proficiency, the individual is rewarded by serious responses from others and may be complimented on his/her question. Some interviewees argue that technical competence may only be exhibited by performing a form of electronic coup counting, e.g., finding loopholes in security or altering a web page.

Interview and observational data indicate that face-to-face and on-line socialization shapes behavior and definitions of hackers and hacking. Both positive and negative reinforcement is conveyed to delineate appropriate and inappropriate behaviors. The most frequent type of positive reinforcement is a serious response to a question posted electronically or asked face-to-face. The question posed (or the technique described) must demonstrate technical proficiency or specificity. Negative reinforcement is manifested as scorn or ridicule for behaviors deemed inappropriate or inept such as vandalism, theft,

destruction, or questions implying a lack of knowledge. Budding hackers engaging in such activities may be labeled "wannabees" or "lamerz."

Neophytes may shape their actions to fit media depictions of hackers. Through list servers and convention sessions, hackers try to send the message that certain behaviors are negatively sanctioned in the electronic community of hackers through "flames." Flames are e-mail messages directed either to the individual or to a group of individuals through a list-server or on an Internet Relay Chat system (IRC). Typically, flames point to the incompetence of the individual and the lack of attachment to the hacker identity. For example, one flame presented on a list-server indicates the more experienced hacker's disapproval of another person (self identified as a hacker) who is boasting. The exchange is as follows:

[original message]: A lot of you guys emailed me and said how dumb and stuff I am and shit but, really. My security is so FUCKING tight that I am never going to get caught (nope never ;) but serious, I do have tight security and no I am not a Fed as one of you suggested that this is a trap *[referring to selling illegal software]*. I'll sell some to dudes at school sometimes, and ONCE, only ONCE, some guy said he was going to report me to the SPA *[Software Publisher's Association--a legal group that enforces software copyrights through litigation]*, so I cracked him one to the nose and told him not to joke about shit like that. I only know a little UNIX shit...If any of you guys are interested in taking me under your wing and teaching me the in's and out's I would like uh do stuff for you, uh or something. You know what I mean...

[one response to message]: my god tell me your joking right. You sound like beavis and butthead combined. get a clue, the key to hacking is learn. learn, learn. you can do that by doing searches on the many search engines. just read everything you can, and always remember no system is secure i don't care what you have guarding/running on it. It's always crackable, and quit the warez shit, it's lame and pointless.

[another response to message]: Who the hell is going to teach you about something you say is shit! No one, just because that shows you don't want to learn how to use it, you just want the power it gives you!

Another example points directly to the possible relationship between media portrayals and the activities of hackers who were responsible for the Amnesty International web page alteration.

[response to the announcement of the Amnesty International Hack: Bloody Hell! We howl and rant and rave when the media portrays us in a bad light, then 'one of our own' goes and does

something exceptionally stupid and insensitive like this. And we wonder where the media gets their idea of malevolent hackers from! If you want to be kewl, whoever you are, go and hack some foreign dictator's homepage, not the homepage of people trying to do some good in the world.

Both cases point to the use of a computer security perspective in evaluating and sanctioning individuals' behaviors. Thus, neophytes learn that activities reported in the mass media are challenged by the majority of hackers.

Novice hackers may be reluctant to forego such activities because the romantic western imagery in media portrayals (the mystique of hacking) contributed substantially to their desire to acquire the hacker identity. A hacker recollects:

Of course there is the romance of the thing too. We all saw War Games, how could that not be fun. Staying up late, talking all night on the fone [*sic*] to people thousands of miles away. It was a rush.

When the thrill seeking extends to vandalism and the novice brags about it, member of the community ridicule them for engaging in status seeking activities, rather focusing on the more individualistic goal of exploration. Whereas, through the exhibition of behavior apparently reflecting approved motives, the novice hacker receives support from experienced hackers.

Novices do not inevitably try to attain status through malicious activities. Most hackers interviewed indicate that no significant change occurred (in their hacking) since they began, but some hackers acknowledge that they previously engaged in malicious behavior. For example, one remembers:

as a kid I thought it was all about 'fucking shit up' and that I was invincible because I was a minor. Now that I'm older and wiser I consider the legal ramifications of everything I do. hacking and otherwise

Those who engaged in these activities early in their hacking careers referred to the mystique of the "computer underground" and their desire to achieve status in it. Some rationalize that their early malicious activities did no real harm as they were often directed toward other hackers who could repair any damage they caused. Overall, those who

identify a shift away from malicious activities claim that they did not recognize the potential consequences of their actions early in their hacking careers.

If people try to seek status in the "computer underground" to validate their hacker identities, the question arises as to whether such an entity exists. Hackers debate whether a computer underground exists as suggested by the media and prior research. Some hackers put it this way:

[the computer underground is a]...self fulfilling prophecy. If the press is looking for a 'computer underground', they will inspire young kids to join an informal 'club', and become one."

The computer underground is just like any other underground. It is probably just a word that is made up to mean everybody who uses computers for less than great purposes for any reason whatsoever.

It does not exist like people think we share all information with anyone interested, so there is no real underground (at least in my opinion).

Others more generally refer to the computer underground as a loose collection of like minded individuals sharing information.

I consider it a place where like minded individuals come to meet. We discuss how to hack and crack as well as the social issues that are pertinent to us. You hear a lot about privacy and exploit scripts...

[the computer underground is]...a loose group of people interested in hacking, phreaking, viruses, carding, or any other topic considered 'fringe.' It's more a term to generally associate all of the above into one category, as dangerous as that may be.

...the computer underground is a pretty vague term...when used by a hacker it usually means hackers/phreakers/warez pups...but in a broader sense I guess it would also include child pornographers, mafia money launderers...and 2 bit criminals (cell phone chippers and the like).

Whatever their position, all hackers interviewed acknowledge that interactions do occur and that through them the rules for hacking are conveyed to others. Whether called an underground or not, hackers engage in enough contact and share enough beliefs to function as a type of electronic subculture or community.

Shared beliefs on freedom of information and the importance of technological progress, and motivations are indications of the community's existence. Yet, most interviewees indicate that the normative boundaries for appropriate hacking activities are

ambiguous. For example, the norm "hack bad things not good things" leaves considerable room for interpretation. Examples of bad things which were hacked (e.g., the Amnesty International hack) are used to clarify boundaries. As one hacker explains his version of the norm:

Hack bad things. Don't hack good things...(example:NOBODY praised the Amnesty International hacker)...Don't hack just so you can enjoy, hack so you can learn, and only destroy things that need to be destroyed...all of these rules are generally picked up and are also from morals.

Other hackers put it this way:

well rules are nothing bad [like] (rm -rf/) unless they are some sicko...and if you are going to hack a website (one of the easy things to do) make sure you got something to say and make sure you are not hacking something good like Amnesty International.

As a general rule, don't attack things that are considered good by hackers or society. Some bastard hacked the Amnesty International home page...that was a bad hack. Why? Because what AI does is good. Hacking the DoJ [Department of Justice] home page is good cuz it made a statement that our government is becoming more facist. And as a general rule of thumb don't hack things that will allow the media to play us off with the 14 year old sociopath image (we hate that...I'm 23, fairly sociable, stable job, engaged, slightly overweight but not unattractive, and generally an alright Joe, so when I see myself being played off as a malicious preteen I get pretty bent)...An example of what not to do would be to hack the White House home page and put up 'Bill Clinton is a stoopid-head' and then proceed to put porn and warez on the server...guaranteed to get us the kind of media coverage we DON'T want...

Bad hacks are, in part, defined as ones which produce negative media coverage. In addition, more experienced hackers attribute malicious activities reported in the media to the lesser experienced novices or wannabees.

Survey data provide support for hackers' assertions that the length of time hacking may play a role in tendencies to engage in more serious activities. Table 13 presents the correlation between activities scale scores and length of time hacking. Unauthorized access, piracy, and deliberate damage scores have significant but moderately weak inverse correlations with the length of time hacking. Thus the more years individuals hack, the less likely they are to engage in deliberate damage, piracy, or unauthorized access. For

Table 13 Pearson Product Moment Correlation Coefficients Matrix
of Length of Time Hacking and Activity Scales.

	Length of Time Hacking (yrs)	Unauthorized Access/Alteration	Piracy	Deliberate Damage	Theft
Length of Time Hacking (yrs)	1.00				
Unauthorized Access/Alteration	-.247***	1.00			
Piracy	-.138*	.345***	1.00		
Deliberate Damage	-.149**	.515***	.306***	1.00	
Theft	-.082	.299***	.282***	.364***	1.00

*p<.10; **p<.05; ***p<.01

individuals reporting one or more instance of serious activities (i.e., deliberate damage and theft), the average length of time hacking is significantly shorter then for those who do not report engaging in such activities (Table 14).

Table 14 Serious Activities by Length of Time Hacking.

Variable	Engage in Activities	N	Mean Length of Time Hacking (yrs)	t-value	df	prob.
Serious Activities	Yes	120	7.337	2.70	88.18	.00
	No	53	10.472			

Identity Importance and Commitment

Study participants vary in the importance they assign to the hacker identity and the amount of time and money spent hacking. For some hackers, "It's not important, it's just who I am." Others point to the importance of hacking in all aspects of their lives explaining that it helped them develop logical thinking skills or expand their interests to other avenues of thought. As one respondent claims:

I get to learn about things that I am extremely passionate about (i.e., computers and phones). I get to challenge myself to certain goals and get personal satisfaction out of having achieved these goals...It has gotten to the point where it [hacking] is totally a part of who I am. It affects things like what I read, what I keep on top of, and who I hang around with even. It's a culture of people that get along with each other despite what their color, religion, or race is.

Importance is also measured by time and money spent on hacking activities. Many claim that they spend a great deal of both their time and money on equipment and books which help them in their hacking activities. One hacker puts it this way:

In all three aspects [time, energy, and money], I've put more into hacking than any other part of my life. My money is always going towards new computers or new equipment. My time and energy is always going towards learning new things and mastering things that I already know.

Respondents employed as computer security professionals found it difficult to separate their work roles and personal hacking activities.

Survey data also indicate patterns similar to electronic interviews on respondents' attachment and commitment to the hacker identity (Tables 15 and 16). The importance

Table 15 Percentage Distributions of Importance of Hacker Identity.

	Strongly Agree	Agree	Disagree	Strongly Disagree	N
I would feel at a loss if I were forced to give up hacking	36.8	45.1	13.7	4.4	182
Hacking is an important part of who I am	26.5	45.3	24.9	3.3	181
Many of the people I know think of me as a hacker	21.4	40.7	29.1	8.8	182
It would not matter to other people that I know if I gave up hacking	8.9	23.3	47.8	20.0	180

(Percentage may not equal 100 due to rounding)

Table 16 Percentage Distributions of Time and Money Spent in Non-Job Related Hacker Activities.

	Not Much	Very Little	Moderate Amount	A Great Deal	N
How much of your time is spent engaging in hacking activities?	7.2	18.2	60.2	13.8	181
How much money have you spent to engage in hacking activities (e.g., books, equipment, etc.)?	13.3	22.2	46.1	18.3	181

(Percentages may not equal 100 due to rounding)

and commitment are exhibited by beliefs such as a loss may be expressed if the individual could not hack, being a hacker is who the person is, and by behaviors such as the expenditure of substantial time and money. The majority of respondents agree that many of their friends identify them as a hacker and disagree that their friends would not be concerned if they gave up hacking; possibly reflecting the importance of hacking as an individual enterprise of self development. Although the majority of survey respondents indicate that being a hacker is important or very important to them (56.9%), interviewees assigned even more importance. The differences may be due to the nature of the question asked.

To further specify the importance of the hacker identity and the attachment to hacking, Table 17 presents correlations between the identity importance, commitment, and motivation (power, skills, challenge) scales. Identity importance and commitment to that identity have a moderately strong, statistically significant correlation. The more important the identity of hacker is to an individual, the more committed the individual. The correlations between identity importance and the motivation scales (power, skills, and challenge) are all moderately weak but statistically significant. The strongest of these indicates that the more importance one places on the identity of hacker the more likely one is to report challenge as an important motivator of hacking activities. Commitment to hacking has the strongest correlation with skills development indicating that the more time and money an individual commits to hacking the more likely that individual is to place importance on skills development.

Regression analyses were performed to identify the models which best accounted for variation in responses (Table 18). Importance of the hacker identity, age, and commitment were predictor variables. Each equation was examined, and the predictor beta with the least significant T score was deleted. Before dropping main effects,

Table 17 Pearson Product Moment Correlation Coefficients Matrix
of Identity Importance, Commitment, and Motivation Scales.

	Identity	Commitment	Power	Skills	Challenge
Identity	1.00				
Commitment	.440**	1.00			
Power	.203**	.129	1.00		
Skills	.209**	.275**	.053	1.00	
Challenge	.311**	.253**	.193**	.173*	1.00

*p<.05; **p<.01

Table 18 Effects of Age, Importance of Identity, and Commitment to Hacking on
Motivational Scales for Hackers

Independent Variables	Skills	Challenge
Age	-.148	
Identity		.810
Commitment	.249	.977
Id*Comm		-1.185
R-Sq.	.093	.158
F*	8.17	9.957
d.f.	2, 160	3, 159
F Full-Reduced	1.090	1.185
d.f.	2, 162	3, 159
Prob. F	>.05	>.05

interactions, and the remaining effects were evaluated to determine whether a significant two-way interaction existed. If one or more significant two way interactions were found, the main effect and its terms were retained in successive equations for further evaluation. A hierarchical analysis was used to evaluate a second series of equations. The full model that included the fully defined highest order interaction term, the complete sets of successively lower orders of interaction terms and the main effects was evaluated. Then each model was systematically evaluated and the highest order term that was not significant was deleted progressively. Two F tests are reported: one for the reduced model and one which compares the full and reduced models under the hypothesis that all omitted coefficients are simultaneously equal to zero.

The reduced skill (motivation) model with age and commitment explained 9% of the variance. This model indicates that the lower a hacker's age the more likely the hacker is to place importance on skills development, and the higher the commitment to hacker activities the more likely the hacker is to place importance on skills development. The reduced challenge (motivation) model with identity importance and commitment explained 15.8% of the variance. The interaction between identity importance and commitment implies that the relationship between the two is, in part, a function of the level of commitment.

Typology of Hackers and Identity Management

The media emphasize maliciousness when describing hackers. Data from hackers emphasize skill development and suggest a desire to negate perceptions of maliciousness. A typology was constructed based on these two dimensions used to describe computing behavior. The first dimension, *degree of maliciousness*, is used by hackers to distinguish between those primarily motivated by exploration or challenge and those primarily motivated by power or financial gain. The media tend to categorize all hackers as being high in maliciousness. The second dimension, *level of skill*, is used by hackers to

distinguish between those exhibiting a depth of knowledge on computer systems and those exhibiting limited knowledge. Again, media accounts tend not to differentiate generally attributing a high level of skill to any hacking activity. These dimensions produce four general types of unconventional computer users (Figure 1).

		MALICIOUSNESS	
		Low	High
SKILL	Low	<i>Novice or Newbie</i>	<i>Wannabees or Lamerz</i>
	High	<i>Hacker (Traditional Hackers or Cyber Explorers)</i>	<i>Crackers (Computer Criminals)</i>

Figure 1: Hacker Typology

Novices or *newbies* have low skill, although they exhibit interest in the unconventional learning of computer systems associated with hackers. The *Hacker* demonstrates high skill and believes in nonmalicious computer exploration. *Wannabees* or *Lamerz* demonstrate low skill and engage in or exhibit interest in learning computer systems to engage in destructive acts (e.g., electronic vandalism). *Crackers* are the computer criminals of media fame; they deliberately commit criminal or destructive acts and have a high level of skill.

Hackers emphasize that self identification, so they have a vested interest in controlling the meaning of the hacker identity. Some individuals believe that hacker has a negative public meaning making them potentially discreditable. Individuals may control information about their hacker identity by adopting a cover when engaged in hacking activities and maintaining a distance between themselves and other hackers. A cover includes the use of a pseudonym in online as well as in face-to-face interactions, providing a degree of anonymity and thus protection from being labeled a hacker. As one hacker

explains, "I have a few friends that know my real name, but this is a small number of people. Most hackers use handles because they want to stay anonymous."

Survey responses indicate the importance of control over the information conveyed about self. Table 19 presents responses to selected items focused on concealment of names and hacker identities.

Table 19 Percentage Distributions on Secrecy of Hackers.

	Strongly Agree	Agree	Disagree	Strongly Disagree	N
I use a pseudonym online so that others will not know my real identity	24.3	42.5	26.0	7.2	181
I am mostly known to other hackers by my pseudonym	27.2	40.6	25.6	6.7	180
I usually don't tell people that I am a hacker	25.8	52.7	16.5	4.9	182
If it comes up in conversation, I will admit to being a hacker	8.8	13.2	55.5	22.5	182

(Percentages may not equal 100 due to rounding)

Anonymity scores are not correlated with identity importance, but anonymity scores are correlated with length of time hacking ($r = -.175$; $p < .05$), i.e., the longer one engages in hacking, the less likely one is to emphasize anonymity. A possible explanation is that the longer the time period one engages in hacking the more likely one is to interact with and be sanctioned by other hackers. (By interacting with other hackers, anonymity may be reduced because handles may become associated with individuals.) Anonymity is also positively correlated with unauthorized access; the more likely the hacker is to engage in unauthorized access, the greater the effort to maintain anonymity ($r = .203$; $p < .001$).

Seeking anonymity is one approach to avoiding stigmatization. Other approaches involve acknowledging the identity of hacker, but distinguish it from the media image of

hacker and creating alternative images. Hackers may distinguish their activities from those of others. They may distance themselves from the negative aspect of the image by adopting a computer security perspective to judge hacking activities. At conventions they may hold sessions focused on media images.

Presentations often focus on values and beliefs deemed important in other cultural contexts. Beliefs associated with the hacker ethic (freedom of information, technological progress) are incorporated into discussions on media treatment. Others draw on Eastern Buddhism, Christianity, Native American, and Nordic beliefs or archetypes. For example, some conventioners and interviewees identified Buddhism as an important source for inspiration. These hackers argue that a loss of ego is fundamental for a focus on the importance of self development and self control, rather than power over other individuals or systems. Drawing on additional archetypes hackers point to the importance of creative power (Nordic myths; Odin), tricksterism and passion (Native American; Coyote), and rebellion (Christianity; Jesus) (Thieme, 1997). Thus, hackers publicly rationalize their behavior and neutralize feelings of guilt for engaging in controversial activities (Sykes and Matza, 1957).

Discussion

During the early phases of the hacker career, the novice hacker seeks direction. Potential mentors emphasize the importance of self direction and development of technical expertise. Media reports focus on the deviant and criminal activities of individuals they call hackers. Depending on those with whom they interact, novice hackers may be encouraged to commit the more devious of hacker activities to gain acceptance and social status as a hacker. Conversely, novice hackers are encouraged to adopt a general set of guidelines, norms for conduct regarding their activities. These norms are often ambiguous and in some instances appear to permit activities considered deviant by those who have been hacking for a while.

Hackers say that as a general rule you only hack "bad things." Yet, examples of good hacks offered included alteration of the Department of Justice page because "our government is becoming fascist." Other interviewees state that the alteration of a web page may be considered a good hack if the alteration is clever. Some avoid defining "good" and "bad" by dismissing the alteration of a web page as demonstrating a low degree of technical proficiency, and thus not an activity of a hacker.

Mass media portrayals of hackers and the social types they invoke may provide a framework for would be hackers to construct their hacker identities. Attributes of heroic and villainous social types which convey intelligence and rebelliousness are used. Although hackers contend that such portrayals are exaggerations, many agree that these portrayals are, in part, based on the activities and attributes of hackers. A romanticized image of both hackers and hacking may entice young individuals. Such individuals may try to establish a hacker identity for themselves by modeling on these attributes. These individuals may engage in activities that are more deviant than the norm as they attempt to attain hacker status. Most hackers may sanction such activities through flames and list server discussions, but some hackers at least implicitly encourage such behaviors helping some novices along a path to a more deviant hacker identity.

Recognition as a hacker is derived from demonstration of technical proficiency (in developing clever programs or finding security loopholes in systems). Some experienced hackers distribute technical information on BBSes or on web pages which neophyte hackers may access. This distribution of information allows individuals with low technical proficiency to engage in activities they believe consistent with a hacker identity. As several hackers complain, individuals currently trying to establish themselves as hackers demonstrate little skill or initiative in learning programming, simply relying on shared information. These hackers fear this democratization of hacking (through sharing) allows persons constructing hacker identities to engage in activities which are at the very least

controversial and at the most destructive, and further to contribute to a negative image of hackers.

Many hackers claim that they are no different from other individuals expressing an interest in technology, but they emphasize rebelliousness in addition to technological competence. The identity is developed through a career beginning with an interest in exploring systems and technology, and proceeding through interaction with others expressing similar interests. Through interaction (often mediated) with others, the novice hacker is introduced to a world of deviant computer usage that begins with the distribution of unauthorized software and technical tricks, but may include activities which are more controversial.

For most experienced hackers, hacking activities remain confined to programming and occasional unauthorized access. These hackers encourage novices to restrict their activities to engage in similar practices. A minority appear to encourage more deviant activities. Neophyte hackers may engage in more deviant activities to establish their technical expertise, to model "role models" described in the media, or to gain recognition. The lack of clear hacking norms may further encourage these wannabees.

Experienced hackers engage in a variety of neutralizing techniques to dismiss the negative aspects of the identity, to avoid stigmatization. These techniques include the control of information about possessing a hacker identity, in-group sanctions through e-mail channels, and the use of culturally valued beliefs to rationalize behavior and neutralize guilt. But these techniques are also problematic for hackers. The anonymity of individuals and the use of pseudonyms may contribute to the mystique of hackers and hacking. This mystique further encourages those individuals with an interest in technology seeking a deviant identity to adopt practices consistent with their understandings of hackers. For most, these understandings will derive from mass media presentations. The

relative anonymity provided individuals through the use of pseudonyms may also reduce the effect of sanctioning in-group deviants through e-mail channels.

In addition to the problems of anonymity, the attachment to and use of beliefs to rationalize behaviors and neutralize guilt by hackers provides them with a faulty position at best. The claims for a uniform hacker ethic further confounds their position in that no evidence obtains that such an ethic exists and, if it does, it runs counter to corporate models. The hacker ethic is the subject of much debate in the hacking community. As early as 1985, many prominent hackers suggested that a uniform ethic does not exist as many hackers imply (Markoff et al, 1985). Instead, these hackers proposed that the similar interests and beliefs of hackers are representative of a hacker "instinct," rather than a uniform ethic (Markoff et al, 1985).

Combined, these problems present a particular dilemma for hackers and their public image. The hacker identity incorporates technological proficiency with independence and rebelliousness. Although the majority of hackers do not commit many of the acts that are attributed to them in mass media accounts, they do engage in activities that deviate from the main stream of computer usage. The lack of clear rules for conduct and a trend toward democratizing technical capabilities found in the hacking community does present a threat to computer systems. Those individuals aspiring to develop a hacker identity based on the media portrayals need not have the technical capabilities that are typically requirements for the hacker identity. As the technical proficiency requirements decrease through innovations of hackers, the potential for greater harm to systems increases. This potential for greater harm represents a threat that hackers themselves have a hand in creating, thus resulting in the potential for an increase in negative media images.

CHAPTER FIVE

CONCLUSIONS AND FUTURE RESEARCH

Summary

Use of components of the interactionist perspective provides the theoretical foundation for studying hackers and their depictions in the media. The identification of social categories or social types to which hackers are assigned in various time periods clarifies the changes which have occurred. Early hackers responsible for much of the technology now used by millions are generally viewed as heroes. The characterization of subsequent cohorts of hackers appears to be predominantly negative ranging from them being seen as at the very least nuisances or at the most serious criminals. By linking the hacker role to another emerging role in the electronic community, i.e., computer security professional, one may see the process of assigning identities, the labeling of groups. The process of labeling involves the power to name as well as the ability to construct identities. For hackers, their social identity is being redefined by computer security professionals' arguments in the mass media and the behavior of some participants in the hacking community.

Social science research on hacking identifies this hacking community as a "computer underground," an important subcultural milieu for the development and conveyance of norms and values central to the hacker identity (Meyer, 1989; Parker, 1976, 1983). Hackers question the existence of something as organized as an "underground." Interview data suggest that electronic channels exist for interaction and norm conveyance. Hacker norms and values are exaggerated forms of norms and values found within the larger cultural framework; for example, beliefs in the freedom of information, (mistrust of) authority, productivity, and individualism exist in distorted and

exaggerated form for hackers. These beliefs promote deviant behavior, if the hacker identity is salient for a person, and norms and values of the subculture are internalized.

In the electronic community of hackers, the status of hacker is contingent on the acceptance and practice of certain activities consistent with the shared definition of hacker. The community/subculture provides opportunities for direct and mediated interaction with others sharing similar interests and attributes. Whether individuals enter the subculture through self or societal selection, they are provided frameworks for behaviors consistent with the internal group identity of hacker. But, the image of hackers is for the most part negative. Individuals may be assigned the hacker label by computer security professionals or law enforcement agents. Yet, only through interaction within the community can behaviors be sanctioned and norms be internalized.

The difference between the computer security perspective as presented in the media and the hackers' perspective is of particular importance. In the media, hackers typically are presented as deviant, if not criminal. Those engaging in hacking activities and who see themselves as hackers are aware that they may be perceived as deviant. Consequently, hackers engage in behaviors to reduce the impact of the deviant label. One response is that hackers try to mentor and otherwise socialize novices' behavior through electronic and face-to-face interaction. Another strategy is to present their perspective on hacking to computer security professionals, government organizations, and mass media organizations.

Conclusions

Four general conclusions may be drawn from this project. First, hackers are diverse but they share many general interests, beliefs, motivations, experiences, and activities. On the basis of these shared characteristics individuals may be placed in or place themselves in the social category of hacker. These characteristics include an interest in learning and skills development, intelligence and independence, a sense of rebelliousness

and self importance, and focus on self interest. In their computing activities, hackers deviate from general norms and some laws regarding computer usage. Such individuals are defined as deviant, and people like them are characterized as a threat to computer systems.

Second, hackers engage in activities which are controversial. Although hacker activities potentially stimulate social change and technological innovation, their technical proficiency and separation from formal control threaten organizations producing computer technology and those who rely on it. They hold many beliefs that promote the democratization of technology, and suggest that these are the reasons for their activities. But, hackers appear to engage in their potentially world changing activities for purposes other than they suggest. Hackers appear to adopt more intrinsic motivations that seem almost self serving. Hackers are also secretive and engage in electronic intrusions that, to them, are nothing more than a complicated "spy game." Although they appear to sanction behaviors that contribute to their negative public image, these beliefs and practices seem to contribute to that negative image, and possibly entice others to engage in activities they perceive to be both deviant and salient to their self image.

Despite problems resulting from the hacker as deviant image, many hackers appear to maintain an attachment to that deviant image. This image imbues a romantic cast to activities which are for the most part mundane. Individuals expressing interest in technology and working in technological fields are considered to be socially inept and often labeled as "geeks" or "nerds." Many hackers try to disavow the hacker as geek image. The romanticized image of hackers invokes characteristics of a rebellious individual with an interest in technology which lies somewhere between the criminal and the geek. Many hackers think of themselves as technological cowboys working to master technology for a greater good against the will of corporations or the government. By drawing on the cowboy (a popular masculine image) and blending it with technological

proficiency, the resulting hacker image is one of mastery through the use of computers. Attachment to this combination of mastery of technology and rebelliousness against the corporate model may contribute to negative images of hackers.

Third, although hackers express concern with the media treatment of their category in the public forum, they also acknowledge their role in the creation of that treatment. Hackers suggest that media accounts are exaggerated and often conflate their activities with the activities of individuals with criminal intent. Some hackers also perceive that computer security professionals, law enforcement, and the computer industry have a vested interest in portraying them as a threat. This vested interest is derived from the need for villains in the electronic realm to provide funding for law enforcement and profit for the computer industry and security professionals. Hackers also acknowledge that members of the electronic community play a role in the creation of this image. Some individuals categorized as hackers either by self or social selection engage in activities which are consistent with those reported in the mass media. Others make exaggerated claims which further contribute to the negative image of hackers.

Fourth, exaggerated claims and activities consistent with media characterizations of hackers are rooted in the typical career of the hacker and contradictions in the hacker identity. The career of the hacker progresses from having a general interest in technology and learning to interacting with others who have similar interests. Through electronic and face-to-face interaction with others, novice hackers learn the characteristics of hackers, and they begin to engage in approved activities, as well as adopt motivations and beliefs consistent with the hacker identity. Those who do not learn or do not accept the general rules of hacking may pursue divergent hacker careers as the more malicious wannabees and crackers. The media portrayals of hackers may serve as models for them. In the future, the hacker identity may undergo change as more individuals adopt it and they may

contribute to both greater threat to computer systems and an even more negative image of hackers.

Problems to Address and Future Research

Three sets of problems need to be addressed in future research. First, the hidden nature of this population coupled with hackers' relative distrust of outsiders was problematic in the early phases of this investigation. Great efforts were made to gain entree into the hacking community and gain the trust of those involved. Difficulties occurred in keeping participants interested in the project, as well as obtaining a convenience sample. Contacting potential participants online also was met with hesitation and distrust, but eventually many self selected to participate. Various hackers at DEFCON V were critical of the survey and elected not to participate. Organizational constraints at DEFCON V also affected survey response rates. Thus, given the nature of sampling problems, generalizations may not be made beyond those participants included in the project.

Second, the electronic techniques used demanded a certain level of technical proficiency to maintain confidentiality and these techniques were not as efficient as I initially believed they would be. Both PGP encryption and anonymous remailers were required for human subjects approval. The use of these techniques was necessary because the potential existed that law enforcement or other hackers might intercept and be capable of identifying participants in the study. Although the use of PGP encryption proved useful, other aspects of electronic interviewing presented problems. I was not able to immediately probe participants. The use of e-mail allowed individuals to take a great deal of time in returning responses despite being sent reminders. The time waiting for responses was often too long in that follow-up questions had to be based on preliminary analyses of the initial questions.

Third, the survey instrument was based on elements of media portrayals and literature that did not provide for many subtleties encountered in this investigation. Questions on the activities of hackers focused more on potentially criminal aspects of hacking, rather than providing insight into more frequent activities of hackers (e.g., programming). Many questions were double barreled in that two electronic means of communication were mentioned in the same question (i.e., e-mail or chat). Other problems included the use of piracy measures and the mention of another convention which may have been annoying to respondents. In addition, respondents complained about the length and breadth of the questionnaire and suggested that future surveys be shorter in length.

Although the general conclusions contribute to a growing body of literature on hackers and hacking, there are many avenues for future investigations into hackers and hacking. More in depth research should be conducted focusing on the career of hackers and the potential role that social types portrayed in the mass media may play in identity construction. More research should be conducted focusing on the computer security relationship with hackers providing detailed accounts from both perspectives. Future research should also be directed to analyses of the emerging electronic community and the basis for trust in these communities. Finally, linkages between the activities of hackers and broader social and economic changes would prove informative in future research.

REFERENCES

REFERENCES

- Abrams, D. and M. A. Hogg. 1990. "An Introduction to the Social Identity Approach." Pp. 1-9 in *Social Identity Theory: Constructive and Critical Advances*, edited by D. Abrams and M. Hogg. (1990). Hemel Hempstead, Hertfordshire: Simon & Schuster.
- Agnew, R. 1995. "Strain and Subcultural Theories of Criminality." Pp. 306-327 in *Criminology: A Contemporary Handbook* 2nd ed, edited by J. Sheley. New York: Wadsworth.
- Barlow, J. P. 1996. "Crime and Puzzlement." Pp. 459-486 in *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*, edited by P. Ludlow. 1996. Cambridge, MA: MIT Press.
- Bequai, A. 1978. *Computer Crime*. Lexington, MA: Lexington Books.
- _____. 1981. *The Cashless Society*. New York: John Wiley & Sons.
- Benson, M.. 1985. "Denying the Guilty Mind: Accounting for Involvement in White Collar Crime." *Criminology*, 23:585-607.
- Berg, B. L. 1995. *Qualitative Research Methods for the Social Sciences*, 2nd ed. Needham Heights, MA: Allyn & Bacon.
- Best, J. and D. F. Luckenbill. 1994. *Organizing Deviance* 2nd ed. Englewood Cliffs, NJ: Prentice-Hall.
- Becker, H. S. 1963. *Outsiders: Studies in the Sociology of Deviance*. New York: Free Press.
- Blake, R. 1994. "Hackers in the Mist." Independent Study Paper from Northwestern University made available through the Electronic Frontier Foundation Homepage; accessed September 1996. (http://www.eff.org/pub/Net_culture/Hackers/Hackers_in_the_Mist.paper).
- BloomBecker, J. 1988. *Introduction to Computer Crime*. 2nd ed. Los Angeles: National Center for Computer Crime Data.
- _____. 1990. *Spectacular Computer Crimes: What they are and how they cost American Business Half a Billion Dollars a Year*. Homewood, Illinois: Dow Jones-Irwin.
- _____. 1989. *Commitment to Security*. Los Angeles: National Center for Computer Crime Data.

- Callero, P. 1985. "Role-Identity Salience." *Social Psychology Quarterly* 48:203-215.
- _____. 1987. "Helping Behavior as Role Behavior: Disclosing Social Structure and History in the Analysis of Prosocial Action." *Social Psychology Quarterly* 50:247-256.
- Cavender, G. 1995. "Alternative Approaches: Labeling and Critical Perspectives." Pp. 349-367 in *Criminology: A Contemporary Handbook* 2nd ed, edited by J. Sheley. New York: Wadsworth.
- Chandler, A. 1996. "The Changing Definition and Image of Hackers in Popular Discourse." *International Journal of the Sociology of Law*, 24:229-251.
- Clough, B. and P. Mungo. 1992. *Approaching Zero: Data Crime and the Computer Underworld*. London: Faber & Faber.
- Cohen, A. K. 1966. "The Delinquent Subculture." Reprinted from *Deviance and Control* by Albert Cohen Pp. 65-66 in *Deviance: An Interactionist Perspective* 2nd ed, edited by E. Rubington and M. Weinberg. (1973). New York: Macmillan Company.
- Collier, P. A. & B. J. Spaul. 1992. "Problems in Policing Computer Crime." *Policing and Society*, 2:307-320.
- Denning, D. 1990. "Concerning Hackers Who Break into Computer Systems." Pp. 137-160 in *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*, edited by P. Ludlow. (1996). Cambridge, MA: MIT Press.
- _____. 1995. "Postscript to Concerning Hackers Who Break into Computer Systems." Pp. 160-163 in *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*, edited by P. Ludlow. (1996). Cambridge, MA: MIT Press.
- Elmer-DeWitt, P. 1995. "Welcome to Cyberspace: What is it? Where is it? And How Do We Get There?" Pp. 6-10 in *Computers in Society* 6th ed., edited by Kathryn Schellenberg. (1996). Guilford, CN: Brown & Benchmark.
- Dunlop, C. and R. Kling. 1991. *Computerization and Controversy: Value Conflicts and Social Choices*. Boston: Academic Press.
- Duff, L. and S. Gardiner. 1996. "Computer Crime in the Global Village: Strategies for Control and Regulation--in Defence of the Hacker." *International Journal of the Sociology of Law*, 24:211-228.

- Elliot, D. 1997. Codebook for National Youth Survey downloaded from ICPSR Archives, Study 08506. (<http://icpsr.umich.edu/>).
- Fialka, J. 1996. "Computer Hackers Cost Big Business \$800 Million in '95." *Wall Street Journal*, June 6, p. B2.
- Fiery, D. 1994. *Secrets of a Super Hacker*. Port Townsend, Washington: Loompanics.
- Fishman, M. 1978. "Crime Waves as Ideology." *Social Problems*, 25:531-43.
- Forester, T. and P. Morrison. 1990. "Computer Crime: New Information for the Information Society." *Prometheus*, 8:257-272.
- _____. 1994. *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*, 2nd ed. Cambridge, Massachusetts: MIT Press.
- Godwin, M. 1996. "Some Property Problems in a Computer Crime Prosecution." Pp. 113-121 in *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*, edited by P. Ludlow. (1996). Cambridge, MA: MIT Press.
- Goffman, E. 1959. *Presentation of Self in Everyday Life*. Garden City, New York: Anchor Books.
- _____. 1963. *Stigma: Notes on the Management of Spoiled Identity*. New York: Simon & Schuster.
- _____. 1967. *Interaction Ritual: Essays on Face-To-Face Behavior*. Garden City, NY: Anchor Books.
- Goldman-Pach, J. 1995. "An Investigation of the Applicability of A General Theory of Crime to Computer Crime." Nonpublished Master's Paper from the University of Arizona from Sociology Express Association Papers.
- Hafner, K. and J. Markoff. 1995. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Touchstone.
- Hastings, D. W., S. B. Kurth, and M. Scholder. 1996. "Work Routines in the Serious Leisure Career of Canadian and U.S. Masters Swimmers." *Avante*, 2:73-92.
- Hearnden, K. 1989. "Computer Criminals are Human, Too." Pp. 415-426 in *Computers in the Human Context*, edited by T. Forester. (1989). Cambridge, Massachusetts: MIT Press

- Hogg, M. A. and C. McGarty. 1990. "Self-categorization and Social Identity." Pp. 10-27 in *Social Identity Theory: Constructive and Critical Advances*, edited by D. Abrams and M. Hogg. (1990). Hemel Hempstead, Hertfordshire: Simon & Schuster.
- Hollinger, R. C. and L. Lance-Kaduce. 1988. "The Process of Criminalization: The Case of Computer Crime Laws." *Criminology*, 26:101-126.
- Hollinger, R. C. 1984. "Computer Deviance: Receptivity to Electronic Rule Breaking." Paper presented at the Annual Meeting of the American Society of Criminology, Cincinnati, OH. November 7. From "Crime by Computer Correlates of Software Piracy and Unauthorized Account Access." R.C. Hollinger. (1993). *Security Journal*, 4: 2-12.
- _____. 1988. "Computer Hackers Follow a Guttman-Like Progression." *Social Science Research*, 72:199-200.
- _____. 1993. "Crime by Computer Correlates of Software Piracy and Unauthorized Account Access." *Security Journal*, 4:2-12.
- Huff, C. and T. Finholt (ed.) 1994. *Social Issues in Computing: Putting Computing in Its Place*. New York: McGraw-Hill.
- Icove, D., K. Seger, and W. VonStorch. 1995. *Computer Crime: A Crime Fighter's Handbook*. Sebastopol, California: O'Reilly & Associates.
- Jenkins, R. 1996. *Social Identity*. New York: Routledge.
- Johson, D. G. 1985. *Computer Ethics*. Englewood Cliffs, New Jersey: Prentice-Hall.
- Johson, D. G. and J. W. Snapper. 1985. *Ethical Issues in the Use of Computers*. Belmont, California: Wadsworth.
- Kim, J. O. and C. W. Mueller. 1978. *Introduction to Factor Analysis: What it is and How to Do It*. Newbury Park, California: Sage.
- Kling, R. (ed.) 1996. *Computerization and Controversy: Value Conflicts and Social Choices*, 2nd ed. San Diego: Academic Press.
- Klapp, O. E. 1962. *Heroes, Villains, and Fools: The Changing American Character*. Englewood Cliffs, NJ: Prentice Hall.
- Kinross, and Render. 1997. Survey of Hackers.
(<http://www.computacenter.co.uk/reports/hackers/results.html>)

- Lemert, E. M. 1967. *Human Deviance, Social Problems, and Social Control*. Englewood Cliffs, NJ: Prentice-Hall.
- Levy, S. 1984. *Hackers: Heroes of the Computer Revolution*. New York: Dell Publishing.
- Lewis, P. H. 1995. "Losses From Computer Breaches Are on the Rise, a Study Finds." *New York Times*, November 20, p. D2.
- Logsdon, T. (ed.) 1980. *Computers & Social Controversy*. Rockville, Maryland: Computer Science Press.
- Lotz, R. E. 1991. *Crime and the American Press*. New York: Praeger.
- Ludlow, P. (ed.) 1996. *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*. Cambridge, MA: MIT Press.
- Markhoff, J., P. Robinson, and E. Shapiro. 1985. "Up to Date." *Byte*, March, pp. 355-356.
- Matza, D., and G. Sykes. 1961. "Juvenile Delinquency and Subterranean Values." *American Sociological Review*, 26:712-720.
- McCaghy, C. H. and T. A. Capron. 1994. *Deviant Behavior: Crime, Conflict, and Interest Groups* 3rd. ed. New York: Macmillan.
- McCall, G. J. and J. L. Simmons. 1966. *Identities and Interactions*. New York: The Free Press.
- Melossi, D. 1985. "Overcoming the Crisis in Critical Criminology: Toward a Grounded Labeling Theory." *Criminology*, 23:193-208.
- Meyer, G. 1989. "The Social Organization of the Computer Underground." Master's Thesis from Northeastern Illinois University made available through the Electronic Frontier Foundation Homepage; accessed September 1996. (http://www.eff.org/pub/Net_culture/Hackers/soc_org_of_comp-underground.paper).
- Nycum, S. 1976. "The Criminal Law Aspects of Computer Abuse: Part I--State Penal Laws." *Rutgers Journal of Computers and Law*, 5:297-332.
- Pagels, H. R. 1984. *Computer Culture: The Scientific, Intellectual, and Social Impact of the Computer*. New York: The New York Academy of Sciences.

- Parker, D. B. 1976. *Crime by Computer*. New York: Charles Scribner's Sons.
- _____. 1983. *Fighting Computer Crime*. New York: Charles Scribner's Sons.
- Pfuhl, E. H. Jr. 1987. "Computer Abuse: Problems of Instrumental Control." *Deviant Behavior*, 8:113-130.
- Pillavin, J. A., and P. L. Callero. 1991. *Giving Blood: The Development of an Altruistic Identity*. Baltimore, MD: Johns Hopkins University.
- Platt, C. 1996. *Anarchy Online*. New York: Harper Collins.
- Quittner, J. 1995. "Hacker Homecoming." *Time*, January 23, 145:61
- Raymond, E. S. and Guy L. Steele Jr. 1994. *The New Hacker's Dictionary, 2nd Edition*. Cambridge, MA: MIT Press.
- Rheingold, H. 1991. *Virtual Reality*. New York: Touchstone Books.
- _____. 1993. *The Virtual Community*. New York: Addison-Wesley Publishing.
- Reinhartz, S. 1992. *Feminist Methods in Social Research*. New York: Oxford University Press.
- Rogers, M. and C. Bogert. 1989. "Red Hackers, Arise!" *Newsweek*, March, 23, 113:58-59.
- Rosenberg, R. S. 1992. *The Social Impact of Computers*. New York: Academic Press.
- Rubington, E. and M. S. Weinberg. 1973. *Deviance: An Interactionist Perspective* 2nd ed. New York: Mac Millan.
- Sandza, R. 1984. "The Revenge of the Hackers." *Newsweek*, December 10, 104:81.
- Schellenberg, K. (ed.) 1996. *Computers in Society*, 6th ed. Guilford, Connecticut: Dushkin Publishing.
- Schiffres, M. 1985. "The Shadowy World of Computer Hackers." *U.S. News and World Report*, June 3, 98:58-60.
- Shea, T. 1984. "The FBI goes after Hackers." *InfoWorld*, June, p. 8.

- Sherizen, S. 1978. "Social Creation of Crime News: All the News Fitted to Print." Pp. 203-224 in *Deviance and Mass Media*, edited by C. Winnick. (1978). Beverly Hills, CA: Sage Publications.
- Sterling, B. 1992. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. New York: Bantam.
- Stoll, C. 1990. *The Cuckoo's Egg*. New York: Simon and Schuster.
- _____. 1995. *Silicon Snake Oil*. New York: Anchor Books.
- Strauss, A. 1997. *Mirrors and Masks: The Search for Identity*. New Brunswick: Transaction.
- Sykes, G. and D. Matza. 1957. "Techniques of Neutralization: A Theory of Delinquency." *Amercian Sociological Review*, 22:667-669.
- Thieme, R. 1997. "Zen and the Art of Hacking." *Internet Underground*, April, 2:27-33.
- Warr, M. 1995. "Public Perceptions of Crime and Punishment." Pp. 15-31 in *Criminology: A Contemporary Handbook* 2nd ed, edited by J. Sheley. New York: Wadsworth.
- Winkler, I. 1997. *Corporate Espionage: What It Is, Why It Is Happening in Your Company, What You Must Do About It*. Rocklin, CA: Prima.

APPENDICES

APPENDIX ONE
MEDIA SOURCES FOR CONTENT ANALYSIS

Articles:

"15 Year Old Hacker Discusses How He Accessed U.S. Military Files." Associated Press article from *The Nando Times*. March 1, 1997. (<http://www.nando.net>).

"\$350 Fine for Swedish Computer Hacker." Reuter Information Service article from *New York Times*, May 1, 1997, p. A4.

"Air Force Computer in Guam Penetrated by Croatian Hackers." Agence France-Presse article from *The Nando Times*, February 21, 1997. (<http://www.nando.net>).

Adams, S. 1996. "How to Keep a Secret." *Forbes*, April 8, 157:108-109.

Alpern, D. and M. Ford. 1983. "Preventing War Games." *Newsweek*, September 5, 102:42-48.

Baig, E. 1996. "How to Practice Safe Surfing." *Business Week*, September 9, pp. 120-21.

Behar, R. 1993. "Surfing the Edge." *Time*, February 8, 141:62-3.

Chandrasekaran, R. 1997. "Hacker Sends 'Bigoted' Note to Erol's Subscribers." *Washington Post*, January 15, p. C10.

"Computer Hacker Made Calls at FBI Expense." *Yahoo News*, February 27, 1997. (<http://dailynews.yahoo.com>).

"Computer Security Experts: Dutch Hackers Stole Gulf War Secrets." Associated Press article from *The Nando Times*, March 25, 1997. (<http://www.nando.net>).

Corley, E. 1989. "Free the Hacker Two." *Harper's Magazine*, September, 279:22-6.

Cortese, A. 1995. "Warding Off the Cyber Invaders." *Businessweek*, March 13, pp. 92-93.

Daly, J. 1996. "John Draper." *Forbes ASAP*, June 3, p. 138.

- Elmer-Dewitt, P. 1993. "Cyberpunks." *Time*, February 8, 141:59-62.
- _____. 1985. "Triumph of a Hacker Sleuth." *Time*, January 28, 125:91.
- _____. 1988. "A Bold Raid on Computer Security." *Time*, May 2, 131:58.
- Fialka, J. 1996. "Computer Hackers Cost Big Business \$800 Million in '95." *Wall Street Journal*, June 6, p. B2.
- Flanagan, W. G. and B. McMenamin. 1992. "The Playground Bullies are Learning How to Type." *Forbes*, December 21, 150:184-9.
- Flohr, U. 1995. "Bank Robbers Go Electronic." *Byte*, November, 20:48.
- Glaser, M. 1997. "AOL 'Hacker Riot' More Like Amateur Hour." *Wired Online*, February 17, 1997. (<http://www.wired.com>).
- Goodman, M. and A. Lynn. 1992. "Hacker for Hire." *People*, October 19, 38:151-53.
- Hackett, G. 1987. "The Hacker Who Vanished." *Newsweek*, January 19, 190:22.
- "Hacker Exposes Weaknesses of Net Construction." Associated Press Article from the *New York Times*, September 13, 1996, pp. D2, D3.
- "Hacker Hits Internet Page of Malaysian Telecom." Reuter Information Service article from *The Nando Times*, February 21, 1997. (<http://www.nando.net>).
- "Hacker Who Broke In AOL is Sentenced to Probation, Home Confinement." Agence France-Presse article from *The Nando Times*, March 28, 1997. (<http://www.nando.net>).
- Hafner, K. 1995. "Kevin Mitnick Unplugged." *Esquire*, August, 124:81-7.
- _____. 1995. "A Super Hacker Meets His Match." *Newsweek*, February 27, 125:61.
- Hitt, J. and P. Tough. 1990. "Is Computer Hacking a Crime?" *Haper's Magazine*, March, 280:45-57.
- _____. 1996. "Terminal Delinquents." *Esquire*, December, 114:175-183, 211-219.
- Hornfischer, J. D. 1995. "Mr. Hacker Goes to Washington." *Omni*, January, 17:31.

- Kempster, N. 1996. "CIA Shuts Internet Site After Hacker Breaks in and Defaces It." *Los Angeles Times*, September 20, p. A25.
- Levy, S. 1984. "The Miserable Life of a Phone Hacker." *Rolling Stone*, September 27, p. 91.
- _____. 1995. "The Case for Hackers." *Newsweek*, February 6, 125:39.
- _____. 1995. "Interview with the Cybersleuth." *Newsweek*, March 6, 125:76.
- Lewis, P. 1995. "Losses From Computer Breaches Are on the Rise, a Study Finds." *New York Times*, November 20, p. D2.
- _____. 1996. "Leading Computer Hacker Strikes Plea Agreement." *New York Times*, April 24, p. A17.
- Marchese, M. 1990. "Digital Desperados." *Scientific American*, September, 263:34-5.
- McGrath, P. and P. Rogers. 1995. "Info Snooper Highway." *Newsweek*, February 27, 125:60-61.
- Meyer, M. 1995. "Is the Hacker Evil or Merely Misunderstood?" *Newsweek*, December 4, 126:60.
- Miller, M. 1986. "Sky High Crime: Busting Captain Midnight." *Newsweek*, August 4, 108:19.
- Moukheiber, Z. 1997. "Cybercops." *Forbes*, March 10, 159:170-72.
- "New Fraud Charges Denied by Hacker." Associated Press Article from the *New York Times*, October 1, 1996, p. A15.
- "Noted and Notorious Hacker Feats." *Byte*, September 1995, 20:151-2
- O'Neil, J. 1996. "Computer Hacker Invades Web Site of the Justice Department." *New York Times (Late New York Edition)*, August 18, p. 33
- Poole, G. A. 1996. "Hack Attack." *Forbes ASAP*, June 3, pp. 97-110.
- Quittner, J. 1995. "Cracks in the Net." *Time*, February 27, 145:44-5.
- _____. 1995. "Kevin Mitnick's Digital Obsession." *Time*, February 27, 145:45.
- _____. 1995. "Hacker Homecoming." *Time*, January 23, 145:61.
- _____. 1996. "Panix Attack." *Time*, September 30, 148:64.
- Ravo, N. 1996. "New Indictment is Filed by U.S. in Hacker Case." *New York Times*, September 27, p. A24.

Recer, P. 1997. "Hackers Sabotage NASA Web Site." Associated Press article from *The Nando Times*, March 6, 1997. (<http://www.nando.net>).

Romero, D. 1995. "A New Force Lurks Amid the Cyber Shadows." *Los Angeles Times*, December 12, p. E1, E6.

Rogers, M. 1983. "The Making of a Hacker." *Newsweek*, September 5, 102:44.

Rogers, M. and C. Bogert. 1989. "Red Hackers, Arise!" *Newsweek*, March, 23, 113:58-9.

Sandza, R. 1984. "The Revenge of the Hackers." *Newsweek*, December 10, 104:81.

Sandberg, J. 1996. "Hacker Introduces the Sound of Silence to Noisy Network." *Wall Street Journal*, September 27, p. B7

"Score one for Hackers of America." *Newsweek*, August 6, 1990, 116:48.

Schwartz, J. 1990. "The Hacker Dragnet." *Newsweek*, April 30, 115:50.

_____. 1992. "Big Guns for Small Targets." *Newsweek*, November 16, 120:63.

_____. 1996. "Hackers Do a Number On the CIA." *Washington Post*, September 20, p. A21.

Shapiro, A. 1995. "Cyberscoop." *The Nation*, March 20, 260:369-70.

Shea, T. 1984. "The FBI goes after Hackers." *InfoWorld*, June, 13:8.

Shiffers, M. 1985. "The Shadowy World of Computer Hackers." *U.S. News and World Report*, June 3, 98:58-60.

_____. 1985. "World of Silver Spy." *U.S. News and World Report*, June 3, 98:60.

Steinberg, S. 1997. "Ex-Hacker Ready for Next Step." *Los Angeles Times*, January 13, pp. D3, D5.

Sussman, V. 1995. "Gotcha! A Hardcore Hacker is Nabbed." *U.S. News and World Report*, February 27, 118:66-7.

Tamaki, J. 1996. "Computer Hacker Faces New Federal Charges." *New York Times*, September 27, pp. B1, B3.

"The Last Adventure of Dark Dante?" *Newsweek*, January 29, 1990, 115:73.

Verity, J. W. 1995. "Hacker Heaven: So Many Computers, So Few Safeguards." *Business Week*, June 26, p. 96.

Wallich, P. 1989. "Hostile Takeovers." *Scientific American*, January, 260:22.
_____. 1995. "A Rogue's Routing." *Scientific American*, May, 272:31.

Wayner, P. 1989. "Goodbye Mr. Chips." *Byte*, October, 14:364.

Young, J. 1996. "Spies Like Us." *Forbes ASAP*, June 3, pp. 71-92.

Television Report Abstracts:

CBS Evening News

"Phone Fraud"	10/3/94	Connie Chung	5:40:20-5:40:40
"Teenage Computer Hackers"	7/17/85	Dan Rather	5:34:00-5:36:30
"Computer Crime/NASA"	12/5/90	Dan Rather	5:50:30-5:50:50
"Computer Hackers"	4/17/92	Harry Smith	5:36:20-5:36:40
"Computer Crime"	8/26/87	Dan Rather	5:49:10-5:52:00
"NC/Computer Hacker"	2/16/95	Dan Rather	5:39:10-5:41:10
"Computer Criminals"	4/3/95	Jim Stewart	5:49:50-5:53:50
"Russia/Computer Hackers"	8/18/95	Dan Rather	5:42:50-5:43:20

ABC Evening News

"Teenage Computer Hackers"	7/17/85	Peter Jennings	5:49:50-5:51:40
"Computer Misuse"	9/26/83	Peter Jennings	6:22:30-6:24:30
"Computer Hackers"	9/15/87	Peter Jennings	5:52:00-5:52:20
"Pentagon Computers"	11/20/91	Peter Jennings	5:37:50-5:38:10
"Computer Spies"	4/25/91	Peter Jennings	5:36:50-5:39:50
"Hacker's Revenge"	12/4/84	Ted Kopel	5:50:10-5:51:50
"Computer Security"	6/5/96	Jack Smith	5:38:50-5:40:30
"W. Germany/Espionage"	3/16/89	Peter Jennings	5:43:10-5:43:40
"Computer Bulletin Boards"	12/22/85	Sam Donaldson	5:12:30-5:15:50
"Computers/Justice Department"	8/18/96	Carole Simpson	5:53:50-5:54:10

NBC Evening News

"USSR Computer Espionage"	3/3/89	Tom Brokaw	5:52:30-5:53:00
"Crime and Punishment"	3/24/92	Tom Brokaw	5:43:20-5:46:50
"Computer Spy Ring"	3/4/89	Connie Chung	5:48:00-5:51:30

"Computer Internet Warning"	2/4/94	Tom Brokaw	5:51:20-5:51:40
"Computer Security"	6/5/96	Tom Brokaw	5:39:10-5:41:30
"MOD Computer Hackers"	7/8/92	Tom Brokaw	5:56:10-5:58:20
"Computer Break-In"	6/22/84	Tom Brokaw	5:39:30-5:41:40
"Computer Theft"	9/21/83	Tom Brokaw	5:43:20-5:47:50
"Pentagon Computers/Hackers"	5/22/96	Tom Brokaw	5:40:40-5:41:10

CNN Evening News

"Computer Internet/CIA"	9/19/96	Bernard Shaw	5:45:10-5:48:10
-------------------------	---------	--------------	-----------------

Movies:

Hackers (1995). Directed by Johnny Lee Miller. Metro Goldwyn Mayer/United Artists.
104 minutes.

Real Genius (1985). Directed by Martha Coolidge. Tri-Star Pictures. 106 minutes.

Sneakers (1992). Directed by Phil Alden. Universal Pictures. 126 minutes.

Tron (1982). Directed by Steven Lisberger. Walt Disney Pictures. 96 minutes.

Wargames (1983). Directed by John Badham. Metro Goldwyn Mayer/United Artists.
110 minutes.

APPENDIX TWO
CONTENT ANALYSIS CODING SHEET

CODING SHEET FOR ARTICLES:

General:

Article Number: _____ Article Date: _____
Author: _____

Newspaper or Magazine Name: _____

If Newspaper==> col. inches: _____; page numbers (e.g. A1, B3,
etc): _____;
wire service: _____

If Magazine==> number of pages _____;

Headline or Title of Article: _____

CATEGORIZATION BASED ON MAJOR FOCUS OF ARTICLE: (Circle the one that best describes this article)

1. -- Computer Security==> Most of discussion focuses on security measures, potential security breaches, how to identify security weaknesses, and how to remedy security problems.
2. -- Computer Development and Technological Progress==> Most of discussion focuses on issues of technological change, changes in the Internet, Education, or the liberating effects of technology.
3. -- Incident Account==> Most of discussion focuses on a specific hacker act or acts, the techniques, the victims, and the hacker or hackers responsible.
4. -- Hacker Focus Story==> Most of discussion focuses on a specific hacker or hackers, sentences for activities, or accomplishments. This may also include stories discussing hackers and their role in the electronic community.

5. -- Other=====> Specify: _____

GENERAL PORTRAYALS OF HACKERS:

(Based on each reference to hacker in the article, list the number of the corresponding image to that reference)

- 1 -- Techno-Criminal=====> Person using electronic means for financial gain. May include references to stolen goods or the term "cyber-thief."
- 2 -- Outlaw/Cowboy/Pirate=====> Computer enthusiasts embodying elements of the romanticized, independent nomads of Western or Pirate folklore. This will usually be prefaced by references to William Gibson in articles (references to wild west and cyberspace as analogous).
- 3 -- Hacker as
 Scientist/Explorer=====> Computer enthusiasts which focus on the intellectual challenge of problem solving. These persons are viewed as explorers pushing back the limits of cyberspace. This will usually be prefaced by or include a reference to hackers of the 1960s and 1970s.
- 4 -- Rebel/Anarchist/Terrorist=====> Person using electronic means to cause damage with the express purpose of making a statement of rebellion or rejection of conventional norms or values. May also include those cases in which calls for changes in the Internet are requested within hacked pages, etc.

5 -- Prankster/Vandal===== > Persons using electronic means to cause damage or service interruption with the intent of playing a joke. May include instances of sending fake e-mail or altering webpages. Should be prefaced in article with reference to the effect of a prank or vandalism. This category is distinct from Terrorist in that no message or demand is made.

6 -- Other===== > Please specify: _____

REFERENCES TO HACKERS:

1. _____	11. _____	21. _____	31. _____
2. _____	12. _____	22. _____	32. _____
3. _____	13. _____	23. _____	33. _____
4. _____	14. _____	24. _____	34. _____
5. _____	15. _____	25. _____	35. _____
6. _____	16. _____	26. _____	36. _____
7. _____	17. _____	27. _____	37. _____
8. _____	18. _____	28. _____	38. _____
9. _____	19. _____	29. _____	39. _____
10. _____	20. _____	30. _____	40. _____

DEFINITIONS FROM ARTICLE (Definitions may include statements like "A real hacker would...." or "Hackers engage in...."==>Implied Defs Okay, just ID them as such):

HACKER: _____

HACKING: _____

COMPUTER

UNDERGROUND: _____

LIST WORDS USED TO DESCRIBE HACKERS OR HACKING:

1. _____ 2. _____ 3. _____ 4. _____

5. _____ 6. _____ 7. _____ 8. _____

9. _____ 10. _____

SPECIFIC TYPES OF CLOTHING, DRUG USE, MUSIC, OR FOOD ASSOCIATED
WITH HACKING OR

HACKERS: _____

OTHER IMPORTANT DESCRIPTIVE ELEMENTS NOT INCLUDED IN ABOVE
CATEGORIES FOUND IN THIS
ARTICLE: _____

SUSPECT/VICTIM IDENTIFICATION:

LIST HACKERS DISCUSSED IN ARTICLE:

NAME AND HANDLE	AGE	CHARGES (IF ANY)
_____	_____	_____

_____	_____	_____

_____	_____	_____

_____	_____	_____

(IF MORE SPACE IS NEEDED, USE THE BACK OF THIS PAGE--MAKE SURE TO INDICATE THAT THE BACK OF PAGE IS USED)

LIST VICTIMS OF ACTIVITIES ATTRIBUTED TO HACKERS:

VICTIM	PROBLEMS CAUSED OR COSTS INCURRED
---------------	--

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

(IF MORE SPACE IS NEEDED, USE THE BACK OF THIS PAGE--INDICATE IF THE BACK OF THIS PAGE IS USED)

TECHNIQUES DISCUSSED IN ARTICLE: (Check all that apply)

- _____ E-mail Attacks (Syn Flood, E-mail Bomb, Send-Mail, etc)
- _____ Viruses or Worms
- _____ Trojan Horses
- _____ Unauthorized Account Access
- _____ Webpage Hack
- _____ FTP Attack (File Transfer Protocol)
- _____ Password Attacks (Sniffing, Password Capture, Password Files Download, etc)
- _____ Social Engineering (Conning Persons, etc.)
- _____ IP Spoofing
- _____ Piracy (Software, Music, or Videos)
- _____ Phreaking (alterations of the phone system in any way)
- _____ Other (please indicate: _____)
- _____ Other2 (please indicate: _____)

MOTIVATIONS OF HACKERS:

CHECK IF PRESENT IN ARTICLE (I=IMPLIED MOTIVATION):

☐ Challenge	☐ Thrill or Excitement	☐ Learning Computer Skills
☐ Power	☐ Recognition	☐ Fun
☐ Cool	☐ Information Collection	☐ Improve Computer Skills
☐ Control	☐ ID Security Problems	☐ Disseminate Information
☐ Money/Legal	☐ Public Awareness	☐ Technological Progress
☐ Self Fulfillment	☐ Terrorism/Anarchy	☐ Theft
☐ Alienation	☐ Boredom	☐ Addiction

OTHER MOTIVATIONS DISCUSSED IN
ARTICLE: _____

HACKERS AND THE MEDIA:

(list no more than 5 quotes about hacking from persons identified as hackers in the article)

NAME/HANDLE--THEN QUOTE ON FOLLOWING LINES

1. _____

2. _____

3. _____

4. _____

5. _____

RESPOND TO THE STATEMENTS BY CIRCLING ONE OPTION FOR EACH QUESTION:

	Strongly Disagree	Disagree	Agree	Stongly Agree
This artical was fair.....	1	2	3	4
This article confused computer crime with hacking.....	1	2	3	4
This article contributes to a negative image of all hackers.....	1	2	3	4

IN REGARD TO THE IMAGES OF HACKERS CONVEYED, THIS ARTICLE MAY BE CLASSIFIED AS:

- 1 Positive
- 2 Balanced
- 3 Negative
- 4 Undecided

IN GENERAL, WHAT LEVEL OF THREAT DO YOU FEEL HACKERS POSE TO COMPUTER SECURITY BASED ON THIS ARTICLE'S PRESENTATION OF HACKERS?

- 1 A Great Threat
- 2 A Moderate Threat
- 3 Low Threat
- 4 No Threat at All

IDENTIFY THE THREATS AND SOLUTIONS PRESENTED IN THE ARTICLE:

HACKER THREAT

SOLUTION

OTHER INFORMATION TO BE INCLUDED:

MAKE SURE TO STAPLE THE ARTICLE TO THE BACK OF THIS CODING SHEET!!!!!!!

APPENDIX THREE
SURVEY INSTRUMENT

This survey is part of a larger investigation into media portrayals of hackers as they compare to actual activities of hackers. Both focus-group and survey techniques are used to identify and address three related issues: 1) media portrayals of hackers; 2) the reliance on such media portrayals in the creation and enforcement of law; 3) the relationship between the first two elements.

This survey is constructed to address three areas of hacking from the perspective of self-identified hackers: 1) general attitudes and opinions on hacking; 2) attitudes regarding media portrayals of hackers and hacking; and 3) practices, motivations, and experiences of hackers.

Completing this survey should take approximately 15-20 minutes. All information collected through this questionnaire will be analyzed in aggregate form and compared to media portrayals. The results of this survey will be incorporated into my Master's Thesis, and will be made available in report form upon completion of all analyses. An announcement will be made on the DC-Stuff List to direct you to a homepage where the results may be found.

Once completed, please return this survey to the box at the information/registration desk marked HUSS-SURVEYS.

Your return of this questionnaire will constitute your informed consent to participate in this study.

SECTION ONE:

The first section of this survey deals with general characteristics of hacking and hackers as reported in prior studies or in the mass media. Please indicate the extent to which you agree or disagree with the following statements.

Strongly Disagree 1	Disagree 2	Agree 3	Strongly Agree 4	
				Hackers have an ethical code.....
				The targets of hackers are most often individuals.....
				Hacking is different from computer crime.....
				Computer crime laws are an over-reaction to media presentations of hackers....
				Violating computer crime laws is necessary to improve computer technologies....
				In general, access to computer systems should be unlimited.....
				Property rights slow the rate of technological change.....

Computer crime laws discourage hacking..... _____
 Law enforcement agencies do not understand the activities of hackers..... _____
 Law enforcement agencies do not understand the motivations of hackers..... _____
 Laws are not necessary to regulate behavior on the Internet..... _____
 In general, hacking is a risky activity..... _____

SECTION TWO:

The second section of this survey deals with your opinions on media accounts, their accuracy, and their importance.

The following statements deal with all printed, television, and movie accounts of hacking. Please indicate the extent to which you agree or disagree with the following statements by placing your answer in the blank provided.

Strongly Disagree 1	Disagree 2	Agree 3	Strongly Agree 4	
				Printed news reports present hacking in a fair manner..... _____
				Printed news accounts confuse computer crime with hacking..... _____
				Printed news reports contribute to a negative image of all hackers..... _____
				Television news reports present hacking in a fair manner..... _____
				Television news reports often confuse computer crime with hacking..... _____
				TV reports contribute to a negative image of all hackers..... _____
				Movies present the activities of hackers in a fair manner..... _____
				Movie portrayals often confuse computer crime with hacking..... _____
				Movie portrayals of hackers contribute to a negative image of all hackers..... _____

The following questions deal with the relationship between hackers and journalists. Please indicate the extent to which you agree or disagree with the following statements by placing your answer in the space provided next to each question.

Strongly Disagree 1	Disagree 2	Agree 3	Strongly Agree 4	
				In general, hackers are concerned with their public image..... _____
				Hackers strive for publicity..... _____
				Hackers attempt to exploit reporters for personal recognition..... _____
				Hackers will exaggerate their activities to reporters to see if they are printed..... _____

The following questions deal with your opinion on the influence various information sources have on public opinion and lawmakers.

In your opinion, how much influence on public opinion of computer crime does each information source have?

No Influence		Some Influence		A Great Deal of Influence
1	2	3	4	5

Printed News Reports (i.e., newspapers, magazines, etc.)..... _____
 Television News Reports..... _____
 Movies..... _____
 Information from Hackers..... _____
 Other (please specify: _____)..... _____

In your opinion, how much influence on the decision making of lawmakers does each information source have in the creation of computer crime laws?

No Influence		Some Influence		A Great Deal of Influence
1	2	3	4	5

Printed News Reports (i.e., newspapers, magazines, etc.)..... _____
 Television News Reports..... _____
 Movies..... _____
 Information from Hackers..... _____
 Other (please specify: _____)..... _____

SECTION THREE:

The third section of this survey deals with your experiences, activities, motivations, and identity as a hacker.

Do you consider yourself to be a hacker? (circle your response)

- 1 YES
- 2 NO (IF NO, PROCEED TO SECTION FOUR)

How important is it to *you personally* to be a hacker? (circle your response)

- 1 VERY IMPORTANT
- 2 SOMEWHAT IMPORTANT
- 3 HIGHLY IMPORTANT
- 4 NOT IMPORTANT AT ALL

Please indicate the extent to which you agree or disagree with the following statements by placing your answer in the space provided next to each question.

Strongly			Strongly
Disagree	Disagree	Agree	Agree
1	2	3	4

Hacking is something I rarely think about..... _____

I would feel a loss if I were forced to give up hacking..... _____

I really don't have clear feelings about hacking..... _____

Being a hacker means more than just hacking..... _____

Hacking is an important part of who I am..... _____

Many of the people I know think of me as a hacker..... _____

Other people I know think that hacking is important to me..... _____

It is important to my closest friends that I continue to be a hacker..... _____

It would not really matter to other people that I know if I gave up hacking..... _____

Please indicate the extent to which you agree or disagree with the following statements by placing your answer in the space provided next to each question.

Strongly			Strongly
Disagree	Disagree	Agree	Agree
1	2	3	4

Only other hackers know that I am also a hacker..... _____

I use a pseudonym on-line so that others will not know my real identity..... _____

I am mostly known to other hackers by my pseudonym..... _____

I usually don't tell people that I am a hacker..... _____

I ask my friends not to tell people that I am a hacker..... _____

If it comes up in conversation, I will admit to being a hacker..... _____

I met my closest friends through e-mail or chat channels..... _____

The people I trust most I met through e-mail or chat channels..... _____

Approximately how long have you been hacking? _____ (years)

At what age did you begin hacking? _____ (years)

Compared to your other non-job activities, how much of your time is spent engaged in hacking activities? (circle your response)

- 1 Not Much Time
- 2 Very Little Time
- 3 A Moderate Amount of Time
- 4 A Great Deal of Time

Compared to your other non-job expenses, how much money have you spent to engage in hacking activities (e.g., books, equipment, etc.)? (circle your response)

- 1 Not Much Money
- 2 Very Little Money
- 3 A Moderate Amount of Money
- 4 A Great Deal of Money

For each of the following statements below write the number which indicates how important the reason is for why you hack:

Very Unimportant 1	Unimportant 2	Important 3	Very Important 4
--------------------------	------------------	----------------	------------------------

- _____ For the Challenge
- _____ For the Thrill or Excitement
- _____ To Learn New Computer Skills
- _____ It Gives me a Sense of Power
- _____ Recognition of Other Hackers
- _____ Because it is Fun
- _____ Because I'm Better at Hacking than Other Activities
- _____ To Improve My Computer Skills
- _____ Because Hacking is "Cool" or "Hip" in the Eyes of Other People I Know
- _____ To Collect Information on Individuals
- _____ To Collect Information on Computer Systems
- _____ It Gives Me a Sense of Control
- _____ To Identify and Report Security Loopholes in Computer Systems
- _____ To Disseminate of Information
- _____ For Technological Progress
- _____ To Make Money
- _____ To Promote Public Awareness
- _____ For Self Fulfillment

Reflecting on how you learned to hack, please indicate the extent to which you agree or disagree with the following statements by placing your response in the space provided after each question.

Strongly Disagree	Disagree	Agree	Strongly Agree
1	2	3	4

Learning to hack:

requires a great deal of self-control..... _____

requires the help of others..... _____

is not difficult..... _____

includes learning social rules for hacking..... _____

Reflecting on your hacking activities from your first to current experiences, please indicate the extent to which you agree or disagree with the following statements by placing your response in the space provided after each question.

Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree
1	2	3	4	5

When I began to hack:

I did not consider the potential legal consequences as much as I do now..... _____

I took more risks with my hacking than I do now..... _____

I was more interested in impressing other hackers than I am now..... _____

I was more malicious in my hacking than I am now..... _____

To compare media portrayals of hackers with the actual activities of hackers, it is also necessary to collect information on your behavior. I'd like to remind you that all surveys are anonymous.

Please give me your best estimate of the number of times you did each of the following things in the past six months:

Never Did This	One to Three Times	Four to Six Times	Seven to Ten Times	More than Ten Times
0	1	2	3	4

acquire another user's password..... _____

use someone's computer account without authorization..... _____

"browse" other person's computer files without authorization..... _____

copy another person's computer files without authorization..... _____

make file modifications in a system without authorization..... _____

- deliberately sabotage another user's programs..... _____
- deliberately "crash" a computer system..... _____
- deliberately damage computer hardware..... _____
- deliberately damage computer software..... _____
- alter the source code of proprietary software..... _____
- make unauthorized copies of proprietary software..... _____
- distribute unauthorized copies of proprietary software..... _____
- receive an unauthorized copy of proprietary software..... _____
- deliberately disrupt services on another computer system..... _____
- introduce viruses or worms into a computer system..... _____
- take computer hardware from another person or organization..... _____
- take credit card numbers from another system or person..... _____
- take money in electronic form from another system..... _____

SECTION FOUR:

I'd like to complete this survey by getting some general information on you.

What is the highest grade you have completed? (check one)

- _____ Grade School (grades 1-8)
- _____ High School (grades 9-12)
- _____ Some College (please indicate number of completed credit hours _____)
- _____ Technical Degree
- _____ College (B.A. or B.S.)
- _____ Graduate or Professional School

What year were you born? 19_____

Which one of these groups best describes you? (check one)

- _____ Caucasian or White
- _____ African American
- _____ Hispanic
- _____ Latino
- _____ Asian
- _____ American Indian/Eskimo
- _____ Other (please specify _____)

Are you:

- _____ Male
- _____ Female

What is your occupation? _____

Which range best represents your individual income for 1996? (check one)

- _____ Under \$10,000
- _____ \$10,000 to \$29,999
- _____ \$30,000 to \$59,999
- _____ \$60,000 to \$89,999
- _____ \$90,000 to \$100,000
- _____ Over 100,000

Thank you for your participation in this survey. As noted in the introduction, this survey is part of a larger project dealing with media portrayals of hackers. If you'd like more information on this project or you'd like to participate in the qualitative focus-groups, feel free to contact me at: sthuss@utkux.utcc.utk.edu

Please return this survey to the box at the information/registration desk marked HUSS. If you have any further comments or suggestions, please feel free to make them in the space provided.

Comments: _____

APPENDIX FOUR
QUALITATIVE QUESTIONS

First Round of Questions:

I'd like to get some general background on everyone to offer some perspective. Without sending information which may identify you personally, tell me a little bit about:

1. Your Education and Occupation
2. Your Interests in Computers
3. How you got into hacking, at what age, and how long you've been hacking
4. What appeal hacking has for you...why do you hack?
5. Your general political beliefs
6. Anything else you'd like to add about yourself

Now, I'd like you to respond to the following questions in as much detail as you wish.

7. What is a Hacker in your own words?
8. What is Hacking? Is it as spectacular as presented in the media?
9. How did you learn to hack?
10. Are hackers computer criminals? Why or why not?
11. What is the computer underground?
12. Is the computer underground a haven for computer criminals?
13. Is hacking an individual activity or is there a collective element to it? If there is a collective element, describe what this element is.
14. Are there social rules for an appropriate hack? If so, generally describe these rules and tell me how you learned these rules.

15. On the whole, the image of the hacker is a negative one. Do you experience any social stigma related to your activities? If so, how do people view you and your activities? Do you tell people that you are a hacker? Are hackers searching for a new, more positive image?

Follow up Questions:

I'd like to explore more fully what it means to be a hacker. To do this, I've come up with the following questions. Some of these questions may seem strange and others may seem similar to the first round of questions, but they will allow me to get a better picture of what hacking is from your perspective.

1. What type of hacker do you consider yourself to be?
2. What have others said about your hacking abilities (positive or negative)?
3. Aside from enjoyment, what do you get from hacking?
4. How important is it to you personally to be a hacker?
5. Compared to other aspects of your life, how much time, energy, and money have you put into hacking?
6. Describe in detail the process you went through in learning to hack.
7. Describe your beliefs regarding the freedom of information. How much of this belief is expressed in your hacking?
8. To what extent do you engage in hacking to gain the acceptance of other hackers? How important or unimportant is the acceptance of other hackers to you?
9. Have your hacking activities changed since you began hacking? Were you more malicious when you began hacking as opposed to now? Did you consider the potential legal consequences of your actions when you began to hack? Are you more careful now than when you began?
10. Describe your beliefs regarding technological progress. How much of this belief is expressed in your hacking?

11. Describe your beliefs regarding centralized authority. Are these beliefs expressed in your hacking? If so, how are these beliefs expressed in your hacking?
12. Are or were you smarter in your classroom experiences than other students? Briefly provide some examples which indicate this aspect of your classroom experiences.
13. To what extent do you feel that law enforcement agencies are interested in cracking down on hackers? Is your opinion based on personal experience? Do you think that current laws reduce hacking activities?

In addition to the questions above, I'd like to present you with three general scenarios. In these scenarios I am taking on the role of either a novice or one who claims to be a hacker. Please respond to the question below as you would normally, if these instances occur.

1. Let's assume that I post a message to a list-server, newsgroup, or BBS announcing that I want to learn to hack.

What is your response to my request?

Would you help me learn?

What advice would you give (e.g., techniques to try or books to read)?

What would I have to do or say to gain your help or support?

2. Let's assume that I post a message to a list-server, newsgroup, or BBS announcing that I am a hacker.

How do you know if I'm a hacker or not?

How would you be able to tell whether or not I know about hacking?

What would I have to do to prove that I was a hacker?

3. Let's assume that I post a message to a list-server, newsgroup, or BBS announcing and say that I am an elite hacker that has just altered a webpage.

How would you respond?

This section deals with your opinions on media portrayals of hackers and hacking (e.g., newspaper, news magazine, television, and movie portrayals). This section will conclude the second round of questions.

1. Do you feel that media portrayals of hackers fairly represent hackers? Why or why not?

2. Is there one media source which is more likely to portray hackers inaccurately than the others? Which media source is this?
3. Please indicate how media portrayals are or are not consistent with your own hacking activities.
4. Do you feel that software industries have a vested interest in portraying hackers as a threat? Why or why not? What is this interest on the part of software industries?
5. Do you feel that the general public has a vested interest in portraying hackers as a threat? Why or why not? What is this interest on the part of the general public?
6. Do you feel that news reporters have a vested interest in portraying hackers as a threat? Why or why not? What is this interest on the part of news reporters?
7. Do you feel that law enforcement has a vested interest in portraying hackers as a threat? Why or why not? What is law enforcement's interest?
8. Do hackers play a role in their negative image? Do some hackers exaggerate their activities to reporters? What effect do you feel this has on the overall image of hackers? What effect do you feel this has on the creation of laws targetting hackers?

VITA

Sean Thomas Huss was born in St. Louis, Missouri in 1967. He attended public schools in Arkansas, and graduated from Arkadelphia High School in 1985. He then attended the University of Arkansas at Little Rock (UALR) until January of 1990. During this period, Sean was the recipient of a music scholarship for his abilities, and joined the Sigma Nu Fraternity where he held many elected positions. He left school in 1990 to take a position with Southern Pacific Railroads as a Senior Agents Accounting Clerk in San Francisco, California. During his tenure with Southern Pacific, Sean maintained his interest in furthering his education by attending classes at Diablo Valley Community College until the summer of 1993.

Sean returned to UALR in the fall of 1993 to complete his Bachelor of Arts degree with majors in both Sociology and Anthropology in the spring of 1995. While completing his degree, Sean served as a statistical teaching assistant, research methods teaching assistant, assistant to the State Forensic Anthropologist, research assistant at the University of Arkansas for the Medical Sciences, and substitute instructor at Remington College. Sean was the recipient of many awards during this period including the John J. Lennon Outstanding Sociology Graduate, Who's Who of American Colleges and Universities, National Dean's List, and membership in the Alpha Kappa Delta Sociological Honors Society. He also presented many papers including an ethnographic study of rural male gossip groups, content analyses of graffiti, and the metaphysical crisis in anthropology, and evaluation of the Liberal Arts program at UALR at the Arkansas Sociological/Anthropological Society meetings.

Sean then entered the University of Tennessee, Knoxville graduate program in sociology the Fall semester of 1995. His current areas of interest include social psychology, criminology and deviance, technology and social change, and research methods. Sean has served as a Graduate Teaching Assistant and Associate since first

enrolling at UTK, and has taught both Introduction to Social Problems and Introduction to Sociology for six semesters. During his tenure, he presented a paper at the Mid-South Sociological Association on graduate teaching assistantship with Laurel Holland. He is currently in the early phases of an investigation dealing with police-citizen exchanges with Kent Kerley. Sean plans to continue graduate work in the UTK Department of Sociology in pursuit of a doctoral degree, and plans to teach and conduct research at the university level upon the completion of the doctoral degree.