HACKING HACKERS

# HACKING HACKERS:

# ETHNOGRAPHIC INSIGHTS INTO THE HACKER SUBCULTURE – DEFINITION, IDEOLOGY AND ARGOT

By

STEVEN WILLIAM KLEINKNECHT, B.A.

A Thesis

Submitted to the School of Graduate Studies

in Partial Fulfillment of the Requirements

for the Degree

Master of Arts

McMaster University

MASTER OF ARTS (2003) McMaster University

(Sociology) Hamilton, Ontario

TITLE: Hacking Hackers: Ethnographic Insights into the Hacker Subculture – Definition, Ideology and Argot

AUTHOR: Steven W. Kleinknecht, B.A. (University of Waterloo)

SUPERVISOR: Professor William Shaffir

NUMBER OF PAGES: vii, 191

## ABSTRACT

While media presentation of hackers and other members of the "computer underground" tend to be pejorative, such representations are often based solely on the viewpoints of "outsiders." As such, society is presented with an image of the hacker subculture that fails to examine the meanings hackers attribute to their activities. Employing symbolic interactionist theory and taking an ethnographic approach to understand the experiences and activities of hackers, this thesis has sought to examine and analyse various characteristics of the hacker subculture. Information pertaining to how hackers define themselves and their activities, the principles underlying the hacker ideology and the distinctive elements of the hacker language constituted the main focus of this thesis. Fifteen semi-structured interviews were conducted with self-defined hackers and fieldwork was undertaken to collect data on and off the Internet during hacker meetings and interactions, and from hacker newsgroups, web sites, and subcultural publications.

Findings from this thesis reveal that the hacker subculture is quite complex and is socially constructed through small-group interactions in various *local* subcultures that, while dissimilar in some respects, identify with characteristics of the *transnational* hacker subculture. Along with the application of role labels, adopting the hacker ideology and argot serve as identifying traits, which are used to situate different subcategories of hackers within the subculture in terms of their status, skill and the perceived ethics of their activities. Condemning "inaccurate" media portrayals of their subculture, imputing labels to others within the subculture to differentiate between "good" and "bad" hackers, invoking the hacker ideology as a vocabulary of motive, and linking their perspective to outsiders viewed favourably by the public, all serve as ways of managing the stigma attached to hackers' deviant public identity. A number of other theoretical and substantive findings, as well as recommendations for future research, are presented.

## ACKNOWLEDGEMENTS

I would like to thank:

My Advisor, Dr. William Shaffir for his constant advice and guidance.

My Committee Members, Dr. Dorothy Pawluch and Dr. Charlene Miall for their time, comments and encouragement.

The participants, without whom this research project would not be possible. Thank you for letting me be a part of your community, for sharing your stories, explanations and insights. Thank you for your openness. Most of all, thank you for all the time you spent meeting and talking with me about your passion, hacking.

Amanda MacGillivary for being so understanding and for supporting me through everything from my initial thoughts to the final submission. Thank you for sparking my creativity and motivating me.

Robert, Laurie and Ryan Kleinknecht, for teaching me to believe that anything is possible.

Dr. Dan Antonowicz and Dr. Roberta Russell for sharing their scholarly wisdom and experiences.

This work is dedicated to: Grandma Stevens and Aunt La for their love and inspiration.

## TABLE OF CONTENTS


CHAPTER ONE: INTRODUCTION ..... 1

GUIDING QUESTIONS ..... 2

LITERATURE REVIEW: A HISTORICAL LOOK AT THE SOCIAL CONSTRUCTION OF THE *HACKER* ..... 3

DEFINING THE COMPUTER HACKER: A HISTORICAL OVERVIEW ..... 4

THE SOCIAL CONSTRUCTION OF HACKERS AS DEVIANTS ..... 7

TOWARDS A STATEMENT ON THE HACKER SUBCULTURE ..... 14

CHAPTER TWO: THEORY ..... 18

SYMBOLIC INTERACTIONISM ..... 18

INTERACTIONISM ONLINE ..... 22

CONCEPTUALIZING SUBCULTURE FROM AN INTERACTIONIST PERSPECTIVE ..... 24

CULTURE FORMATION: THE SUBCULTURAL MOSAIC ..... 25

THE PROCESSUAL NATURE OF SUBCULTURE ..... 28

SUBCULTURAL VARIANTS ..... 31

CHARACTERISTICS OF SUBCULTURE ..... 32

CHAPTER THREE: METHOD ..... 35

ETHNOGRAPHIC INQUIRY ..... 35

INTERACTIONISM AND ETHNOGRAPHY ..... 36

DEALING WITH PRECONCEPTIONS ..... 37

LOCATING INFORMANTS AND DECIDING UPON THE RESEARCH SETTING ..... 41

NEGOTIATING PRESENCE AND SELF-PRESENTATION IN THE FIELD ..... 47

COLLECTING DATA ONLINE ..... 59

DISCUSSION ..... 62

CHAPTER FOUR: TOWARDS A DEFINITION OF HACKER: HACKER AS A CONTESTED TERM ..... 65

HACKERS VS. THE MEDIA: CHALLENGING MEDIA DEFINITIONS OF "HACKER" ..... 68

CONTESTED INSIDER DEFINITIONS OF "HACKER" ..... 73

HACKERS AND CRACKERS ..... 76

HATS: WHITE, BLACK AND GREY ..... 81

DISCUSSION ..... 86
CHAPTER FIVE: THE HACKER IDEOLOGY ..... 91
CONCEPTUALIZING IDEOLOGY ..... 91
THE HACKER SPIRIT ..... 93
THE HACKER SPIRIT: THE PURSUIT OF KNOWLEDGE ..... 95
PRINCIPLE #1: HIGHER UNDERSTANDING REQUIRES AN UNORTHODOX APPROACH ..... 97
PRINCIPLE #2: HACKING INVOLVES HARD WORK ..... 98
PRINCIPLE #3: HACKING REQUIRES A "LEARN FOR YOURSELF" APPROACH - LEARN BY DOING ..... 100
PRINCIPLE #4: SHARE YOUR KNOWLEDGE AND INFORMATION WITH OTHERS ..... 102
PRINCIPLE #5: YOU'RE EVALUATED BASED ON WHAT YOU KNOW AND YOUR DESIRE TO LEARN ..... 106
PRINCIPLE #6: MISTRUST AUTHORITY ..... 108
PRINCIPLE #7: ALL INFORMATION SHOULD BE FREE ..... 114
DISCUSSION ..... 118
CHAPTER SIX: HACKER ARGOT ..... 126
CONCEPTUALIZING ARGOT ..... 126
THE HACKER LANGUAGE: TECHSPEAK AND JARGON ..... 130
TECHSPEAK ..... 134
JARGON ..... 138
NETSPEAK AND THE CONVENTIONS OF ONLINE TALK ..... 139
L3375P34K ..... 147
ROLE LABELS ..... 155
DISCUSSION ..... 158
CHAPTER SEVEN: CONCLUSION ..... 163
SUMMARY ..... 163
THEORETICAL AND SUBSTANTIVE CONTRIBUTIONS ..... 168
DIRECTIONS FOR FUTURE RESEARCH ..... 177
BIBLIOGRAPHY ..... 179
APPENDIX A: CODING SHEET ..... 188
APPENDIX B: "THE CONSCIENCE OF A HACKER" ..... 190

## LIST OF DIAGRAMS AND TABLES

DIAGRAM 1. DEFINITIONAL SHIFT ..... 4
TABLE 1. IRC CHAT "TRANSLATED" ..... 141

# CHAPTER ONE

# INTRODUCTION

What is a hacker? As Taylor (2001) points out, over the course of the last forty years the word "hacker" has become a highly contested term. In recent years the media have solidified the notion of hacker to mean someone who gains "...unauthorized access to, and subsequent use of, other people's [computer] systems" (Taylor, 2001, p. 284). However, "hacker" has not always been synonymous with deviant behaviour, at least not of the criminal sort. The term was first coined at the Massachusetts Institute of Technology (MIT) in the 1950s and 1960s to denote the highly skilled but largely playful activity of academic computer programmers searching for the most elegant and concise programming solution to any given problem (Levy, 1984). Three generations of hackers later, and the term is almost exclusively used to depict people who engage in the illicit use of computers.

While media presentations of hackers and other members of the "computer underground" tend to be fairly pejorative, such representations are often based solely upon the viewpoints of "outsiders" (e.g., politicians, law enforcement officials, computer security personnel). As such, society is presented with an image of the hacker subculture that fails to account for the meanings hackers

attribute to themselves and their perspectives. By engaging in participant observation among self-defined hackers and conducting in-depth interviews with them, the goal of this thesis is to offer an ethnographic examination and analysis of the hacker subculture.

## GUIDING QUESTIONS

At the outset of this project, I had decided upon two broad guiding questions to be used throughout the course of the research. They included, (1) how do people become involved in the hacker subculture and, (2) what characterizes the hacker subculture? However, a third question regarding how "hacker" was defined, developed as I met with hackers and began reading the literature (both scholarly and media produced) pertaining to hackers. As an ethnographer venturing into the foreign world of the hacker, I decided from the beginning to let hackers define what the term meant to them. In so doing, I quickly realized that mainstream representations of hackers tended to over-simplify the term and were often in opposition to those definitions applied by the people with whom I had been meeting. Thus, how hackers define the terms *hacker* and *hacking* in comparison to outsiders' understandings became significant.

In attending to these questions a series of interactionist concepts have been applied and investigated to offer a sociological perspective grounded in the life-world experiences and perspectives of hackers. In particular, the concept of

subculture has been examined and applied to the offline (i.e., real-world)[1] and online aspects of hackers' lived experiences. While there is extensive qualitative literature examining people's real-world subcultural experiences (e.g., Becker, 1963; Fine, 1983, 1987; Humphreys, 1975; Letkemen, 1973; Liebow, 1967; Mitchell, 1983; Prus & Irini, 1980; Whyte, 1943), the Internet has provided a new medium through which people interact and develop virtual communities. A growing body of scholarly literature is developing as academics seek to offer an understanding of the human lived experience as it pertains to the new technologies. I hope to contribute to this material by examining how various aspects of the hacker subculture are formed and mediated through their online interactions.

## LITERATURE REVIEW: A HISTORICAL LOOK AT THE SOCIAL CONSTRUCTION OF THE *HACKER*

Of substantive interest to this project is the social scientific research that has been conducted on the hacker subculture. Although the (computer) hacker culture has been in existence since the 1950s, there has been little in the way of scholarly literature published on hackers. However, in the context of growing governmental, commercial and public concern regarding computer security an increasing amount of social research was conducted from the late-1980s to

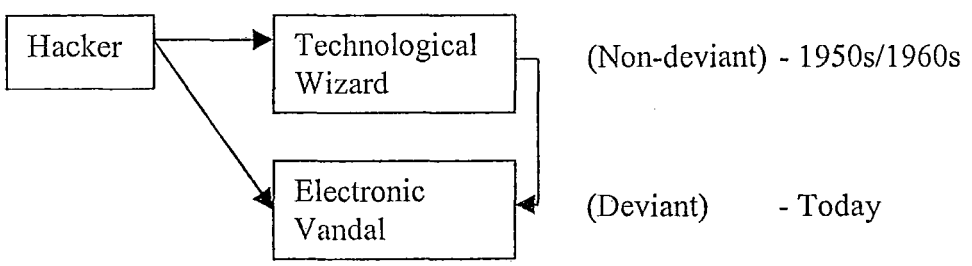
[1] The terms "offline" and "real-world" have been used interchangeably in this report to denote activities that transpire in the physical world in which we live. In contrast, the word "online" has been used to describe those activities that take place over a computer network, such as the Internet or a Bulletin Board System. The term "virtual" refers to anything that has been created by or mediated through a computer software program. The notion of representing oneself in a virtual space, such as "on" the Internet or telephone system, necessitates that these distinctions be made.

present. For the most part, the literature focuses on describing and analysing the history and social construction of hackers and the term *hacker*. To a lesser degree, these studies also examine characteristics of the hacker subculture such as their beliefs and ideology, identity, patterns of behaviour, and motivations. While research on characteristics of the hacker subculture will be presented in later chapters, the focus of the literature review in this section is on providing an overview of findings pertaining to the history and social construction of hackers.

**Defining the Computer Hacker: A Historical Overview**

As a number of researchers (see Arbaugh, 1999; Chandler, 1996; Clough & Mungo, 1991; Copes & Huss, 1999; Duff & Gardiner, 1996; Hafner & Markoff, 1991; Huss, 1998; Taylor, 2001) have indicated, the term hacker has undergone a number of definitional shifts since the 1950s. Through a process of re-definition the meaning associated with the term *hacker* was transformed in the popular discourse from non-deviant to deviant. Although the hacker was once seen as a "technological wizard", the term is now taken by and large to mean "electronic vandal" (see Diagram 1).

Diagram 1. Definitional Shift



The first generation of hackers was comprised of the highly skilled computer programmers at MIT in the 1950s and 1960s who delighted in finding the most ingenious ways of overcoming programming obstacles (Chandler, 1996; Levy, 1984; Rheingold, 1991; Taylor, 2001; Turkle, 1997). As major contributors to the development of the personal computer and pioneers of what was later to become the Internet, hackers were held in high esteem for their devotion, creativity and skill. Considered among the brightest in their field, the term hacker became synonymous with being a "technological wizard" or "computer virtuoso" (Chandler, 1996; Clough & Mungo, 1992; Taylor, 2001; Turkle, 1997). To be a hacker was to wear a badge of honour - the label being one of the highest compliments of computer programming genius a person could receive (Hafner & Markoff, 1991; Arbaugh, 1999).

The second generation of hackers was responsible for bringing computer hardware to the masses (Chandler, 1996; Clough & Mungo, 1992; Levy, 1984; Rheingold, 1991; Taylor, 2001). Entrepreneurial computer radicals such as Stephen Jobs and Stephen Wozniak, founders and designers of the Apple personal computer, characterized the second generation of hackers (Chandler, 1996; Clough & Mungo, 1992; Huss, 1998; Rheingold, 1991). With the goal of bringing "the same power over information that large corporations and the government have over people", the marketing of the Apple personal computer echoed the counterculture and "power to the people anthem of the Sixties" (Clough & Mungo, 1992, p. 32). So successful were Jobs and Wozniak in

bringing the personal computer to the public that by 1980 they had a combined worth of approximately $US 400 million (Chandler, 1996) as Apple Computer Corporation moved from selling $US 2.5 million worth of PCs in its first year of operation in 1977 to $US 583 million in 1982 (Duff & Gardiner, 1996). As Huss (1998) points out, "The label hacker served as a positive label of accomplishment and the potential for economic success for this second wave" (p. 11).

Inheriting the personal computer technologies of the previous generation, the third generation of hackers became defined by those leading the way in the development of the latest video game architecture (Chandler, 1996; Clough & Mungo, 1992; Levy, 1984; Taylor, 2001). However, as Chandler (1996) points out, during this era of innovative software development, individuals began to take advantage of their knowledge of computer programming to "pirate"[2] software (Chandler, 1996). Thus, with this generation, the term hacker can be seen as not only involving the intense computer programming that defined first and second generations, but also the use of computer knowledge to break copyright protections and unauthorized sharing of proprietary software.

The fourth generation of hackers became ever more characterized by criminal behaviour as a growing number of individuals were seen as becoming involved in not only the pirating of computer software, but also the construction and spread of computer viruses (Chandler, 1996; Clough & Mungo, 1992). As wide area networks such as Bulletin Board Systems and, more recently, the

[2] *Pirating* involves making, giving or receiving an unauthorized copy of proprietary software.

Internet became increasingly widespread the term hacker has come to describe both the computer network gurus responsible for network operation and development, and also those involved in the illicit access of computers on local and wide area networks (Taylor, 2001).

**The Social Construction of Hackers as Deviants**

Following this historical overview, the question for researchers focuses on how hackers came to be defined as deviant. The principal argument is that the explanation has to do with who holds the power in the claims-making process and the social milieu within which the process was (and still is) occurring.

In her writing on social constructionism, Donileen Loseke (1999) indicates that *who* is doing the defining (i.e., the status of the claims-maker) can have a significant impact on the success or failure of a claims-making initiative. In the eyes of the public some types of claims-makers and evidence hold particular sway. Loseke (1999) argues that, in general, scientists and others possessing "lofty academic credentials" are particularly influential. The research identifies three main groups of claims-makers who were influential in the construction of the hacker as deviant: (1) the computer security industry (CSI); (2) government officials; and, (3) the media.

Given that members of the CSI have particular expertise in the area of computers and electronics, they are situated fairly well in what Loseke (1999) refers to as "the claims-making hierarchy." Since they are also entrusted with protecting public and corporate computer systems from "hacker" intrusion, their

claims against hackers are given further credence (Huss, 1998; Jordan & Taylor, 1998; Taylor, 1999, 2001). The CSI's relationship with lawmakers and corporations provides them with even greater occupational power to define hackers as deviant (Copes & Huss, 1999). Copes and Huss (1999) contend that nearly all CSI professionals see hacking as a threat, with hard line computer security specialists advocating that, "...an intensive effort must be made to define the activities of hackers as unethical, unacceptable, and criminal" (p. 13). By stigmatizing hackers as deviant, members of the CSI are able to distance themselves from hackers, reaffirm their professional identity and thus, help to ensure the continuity of their profession (Huss, 1998; Taylor, 1999, 2001).

The role played by politicians in the claims-making process is also emphasized (Chandler, 1996; Rosoff, Pontell & Tillman, 1998; Taylor, 1999; 2001). Given their function of enacting laws and protecting the public, any claims made in keeping with this agenda will be seen as particularly influential by society. Taylor (2001) utilizes information taken from the United Kingdom's debates on the Computer Misuse Act, a piece of "anti-hacking" legislation, to illustrate how politicians' law-making role can be seen as claims-making activity contributing the definition of hackers as criminals.

The third group identified in the literature are the media (Chandler, 1996; Copes & Huss, 1999; Duff & Gardiner, 1996; Huss, 1998; Rosoff et al., 1998; Taylor, 1999, 2001). While some media accounts present a balanced picture of the hacker subculture, the overwhelming consensus within the literature is that

most media portrayals of hackers are overly sensationalistic. Rosoff, Pontell and Tillman (1998) argue that media sensationalism combined with the timing of particular hacker antics, such as the spread of computer viruses and the apprehension of their creators, have captured the public's imagination. In keeping with its agenda to attract the public's attention by presenting "newsworthy" stories, Huss (1998) argues that, "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" (p. 1). His research suggests that for a story to be "newsworthy" it must reflect, "timeliness, prominence, novelty, or, for crime and deviance stories, the seriousness of the incident" (1998, p. 20). Therefore, the public is presented with the most spectacular stories about "hackers." As Copes and Huss (1999) suggest, this type of unbalanced presentation of the hacker misleads people into thinking that hackers are the source of all computer crime.

The literature highlights a number of strategies used by politicians, the CSI and the media to influence public perception about hackers, including: (1) drawing clear distinctions between conformists and deviants; (2) using imagery which equates hackers with the "abnormal" (e.g., monsters, addicts); (3) linking the "problem" of hacking to other more established social problems; (4) presenting hackers as being physically dangerous and thus, requiring restraint in their apprehension; and, (5) playing to audience's emotion of fear.

Taylor (2001) states that one strategy used by politicians during parliamentary debate concerning British anti-hacking legislation was to draw very clear lines between "us" (i.e., conformists) and "them" (i.e., deviants). In this case politicians reinforced group identity by outlining the positive qualities that produce "us" while simultaneously emphasizing the alien nature of "them." For example, one politician in the debate made reference to a leading bank official who had taken the time to write the MP asking him to support the new anti-hacking legislation. The MP contrasted the personal qualities of the constituent with hackers by discussing a hacker's posting to a computer bulletin board. In the posting the hacker makes reference to assassinating another MP for supporting the legislation. This example is also a good illustration of how the claims-makers appeal to their audience's emotion of fear in order to generate support for their claims. Other extreme cases are referenced by politicians such as the hacker who allegedly tried to kill hospital patients by accessing their drug records and altering their prescriptions (Chandler, 1996; Taylor 2001).

As a number of constructionists (see Ibarra & Kitsuse, 1993; Loseke, 1999; Spector & Kitsuse, 1987) have indicated, it is necessary for the analyst to pay close attention to the words used by claims-makers in their attempts to persuade audiences. Researchers examining how hackers came to be defined as deviant also make this point by drawing attention to the pejorative rhetoric used by politicians and CSI personnel (Chandler, 1996; Huss, 1998; Taylor, 2001). For example, Taylor (2001) argues that words such as "rat", "monster", "vandal", and

"bastard" are used by CSI writers in books and journal articles to distance themselves from hackers and emphasize hackers' deviant and dangerous qualities. Chandler (1996) also discusses the language used by claims-makers to define hackers as deviant. Loaded terms such as "addict", "compulsive", and "obsessive", used to describe hackers' willingness to spend hours on their computers and their intense drive for exploration, paint a picture of mentally disturbed individuals no longer in control of their behaviour (Chandler, 1996). These terms, along with others such as "monster", "abnormal" and "robot" portray hackers not only as mentally unstable, but also non-human and dangerous (Chandler, 1996).

Another strategy used by claims-makers is to relate hacking to other more established social problems such as the underground distribution of pornography and drug use (Chandler, 1996; Taylor, 2001). Chandler (1996) identifies five predominant images used in the media to characterize hackers. These images include: (1) cowboys; (2) intellectual joyriders; (3) murderers; (4) mentally ill; and, (5) spies. While the more positive cowboy metaphor conjures up feelings of individualism and freedom, hackers are more often portrayed in terms of the dangerous and potentially subversive characteristics associated with the other types of images. Drawing on headlines such as "Intellectual Joyriders' Jailed", Chandler (1996) argues that by grouping the escapades of joyriding youth racing about in stolen cars together with hackers and their "illegal computer joyriding", the media alerted the public to the danger of computer hackers and contributed to

the moral panic surrounding their alleged activities. As another example, Chandler (1996) discusses how media reports liken computer viruses to AIDS. She states that, "...linking two 'folk devils' in this way, lends truth to media speculation and reporting about both because reports on AIDS can now be compared with hacking and vice versa, and in this way spurious evidence becomes corroborative" (p. 241).

Vivid visual cues are also employed by legal officials via the media to illustrate the dangerousness of hackers. Taylor (2001) argues that images of police raids on suspected hackers' homes can be interpreted as exhibiting the displaced fear of the law enforcer or as a deliberate strategy to increase hackers' deviancy status. In addition, Taylor (2001) points out that politicians' lack of evidence concerning the claims made against hackers (e.g., their use of drugs, trafficking child pornography) helps to buttress the success of their claims by again playing on audience fear. While politicians lack specific evidence, rumour and guesstimates increase pressure to legislate against hackers because of the fear that is produced by the unknown. However, if we are to understand how politician's and the CSI's claims have been successful, Taylor (2001) also argues that it is necessary to consider the socio-historical context in which they were made.

Employing Marshall McLuhan's notion of "cultural lag", Taylor (2001) posits that there is an air of mystery surrounding technology in our society. He states that, "...hackers are perhaps a specific illustration of some of the wider

problems society faces as it struggles to assimilate new information technologies into existing social structures" (2001, p. 285). He argues that the ongoing computer revolution, combined with privatization of consumption, post cold-war feelings of vulnerability and the information/generation gap, has led to conditions of large-scale social and technical transition where hackers are made the scapegoats of the social unease accompanying this transition. It is within this context that claims-makers are able to persuade their audience.

Taylor (2001) also maintains that the non-physical nature of hacking, along with its anonymity and (popularly defined) illicit nature, combine to create an air of mystery surrounding the activity, which in turn contribute to societal fear and anxiety. He indicates that these factors make it easier for the media to portray hackers in deviant terms.

Those making counter-claims against the media, CSI, and politicians include hackers and those acting on their behalf (e.g., defence attorneys). In an attempt to contest the assertions made against them a claim employed by hackers is that of similarity. One such similarity hackers maintain they share with members of the CSI is the desire to explore and test the limits of technology (Taylor, 2001). Given the CSI's attempt to professionalize their work, hackers have been largely unsuccessful in employing this claim (Taylor, 2001). That is, since the public sees hackers as deviant, those in the CSI avoid public disclosures that would associate members of their burgeoning industry with "computer criminals." A further counter-claim used by hackers is to assert that authorities

are over-reacting and that hackers are simply misrepresented by the media and other claims-makers (Huss, 1998; Taylor, 2001). Counter-claims made by hackers and those acting on their behalf are largely unsuccessful. Such appeals must be made within a social atmosphere wherein hackers have been predefined as deviant. Therefore, the majority of the populace are unsympathetic to individuals who are seen as having contravened the legal conventions of society. Given their inability to influence popular discourse surrounding hacking, Huss (1998) suggests that traditional hackers have lost control of the popular definition of the hacker image.

## TOWARDS A STATEMENT ON THE HACKER SUBCULTURE

> *We can describe the perspectives of one group and see how they mesh or fail to mesh with the perspectives of the other group: the perspectives of rule-breakers as they meet and conflict with the perspectives of those who enforce the rules, and vice versa. But we cannot understand the situation or process without giving full weight to the differences between the perspectives of the two groups involved. It is in the nature of the phenomenon of deviance that it will be difficult for anyone to study both sides of the process and accurately capture the perspectives of both classes of participants. (Becker, 1963, p. 173)*

It is not within the purview of this thesis to acquire, first-hand, the perspectives of both insiders and outsiders to the hacker subculture. As Becker (1963) suggests, such an undertaking is not practical considering the amount of time necessary to gain access to and win the confidence of the people we hope to study. Therefore, what is presented is necessarily a one-sided perspective on the things considered important to one group and not the other. The focus within this

section and those that follow is on the perspective of hackers, and not outsiders. With that said, two qualifications must be made. First, the perspectives of outsiders are necessarily taken into account by hackers in coming to a sense of what defines them. Such understandings are made clear in how hackers interact with one another, but more importantly in how they present themselves to outsiders. These insider perspectives, however, are presented through the lens of the hacker rather than through the perspective of those labelling hackers as somehow different or deviant from an outside vantage point. Second, outside perspectives are taken into account to a certain degree in this thesis by relying upon secondary source materials such as previous research and media presentations. The need to understand a subculture from the standpoint of those involved in its development warrants the focus on one group, at the expense of another.

As Huss (1998) points out, most of the information we have about hackers is based upon media portrayals. A difficulty one encounters when trying to understand hackers through the media is that, as discussed, the media offers a representation of hackers that is necessarily limited due to their outsider status and focus on producing newsworthy stories. Very few studies have gone directly to hackers as the primary source of data on their experiences, viewpoints and

activities.[3] Departing from much of the previous research, I work from the symbolic interactionist perspective (Blumer, 1969; Mead, 1934; Prus, 1996) and rely upon ethnographic fieldwork and in-depth interviews to acquire an insider perspective into the life-worlds of hackers.

The notion of "subculture" is central to my work. Prus (1997) defines a subculture as, "a set of interactionally linked people characterized by some sense of distinctiveness (outsider and insider definitions) within the broader community" (p. 41). He indicates that, "subcultures typically develop around some form of activity, but imply reflectivity, interaction and continuity over time" (1997, p. 41). The concept of subculture will be examined further in the next chapter.

Drawing and abstracting from various researchers' theoretical writings on subculture (e.g., Arnold, 1970; Clarke, 1974; Fine, 1987; Fine & Kleinman, 1979; Goode, 1957; McCaghy & Capron, 1997; Prus, 1997; Shibutani, 1955), some of the main features characterizing a subculture can be said to include: (a) an ideology shared by members of the community; (b) common patterns of activity that distinguish those within the subculture from outsiders; (c) a unique language or argot that is particular to the subculture; (d) symbolic objects or artefacts that

[3] Arbaugh (1999), Huss (1998) and Taylor's (1999, 2001) research are notable exceptions. Huss (1998) combines both quantitative and qualitative research techniques to analyze the social construction and labelling of hackers and the hacker identity. He bases his findings on media, computer security industry and hacker perspectives. Arbaugh (1999) bases his research on online interactions with and between hackers and examines hacker-produced information (e.g., newsletters, magazines, tutorials) to delineate the different roles played by members of the computer underground (e.g., hackers, crackers, phreaks, warez d00dz, lamers). Similar to the current thesis, Arbaugh (1999) examines whether or not the computer underground can be classified as a subculture. Taylor's (1999, 2001) research compares hackers' and the CSI's perspectives by interviewing and analysing each side's accounts.

hold unique meaning to those within the subculture; (e) community norms or rules of behaviour; and, (f) self-image/identity which is closely linked to the subculture's ideology. The ensuing discussion will focus on examining the hacker subculture in terms of its ideology and argot. Additional chapters explore how the term hacker and hacking are defined by outsiders and insiders and discuss some of the methodological issues surrounding online field research. This thesis very much represents a departure in certain ways from examining hackers in terms of their associated criminally deviant characteristics. Moving beyond what Prus (1997) has termed the "deviance mystique" the ultimate goal of this report is to present an interactionist account of hackers' perspectives as they are shared with others and enacted in the here-and-now of online and real-world experience.

Before moving on to the substantive content of this paper, an overview of the theoretical framework and methodological approach is presented in order situate the reader and frame the current analysis.

# CHAPTER TWO

# THEORY

This chapter and the one that follows present the theoretical and methodological approach taken to investigate the hacker subculture, while at the same time offering insights into the types of theoretical and methodological issues that had to be dealt with along the way. In order to fully appreciate how human group life is accomplished on an everyday basis, I have adopted a symbolic interactionist perspective (Mead, 1934; Blumer, 1969; Prus, 1996, 1997) and used an ethnographic approach (Prus, 1996, 1997) to study the experiences of those within the hacker community. As will be made clear in these next two chapters, the theory and method used in this study are not wholly separable.

## SYMBOLIC INTERACTIONISM

In general, symbolic interactionism can be described as, "...the study of the ways in which people make sense of their life-situations and the ways in which they go about their activities" (Prus, 1996, p. 10). According to Herbert Blumer (1969), symbolic interactionism rests on three basic premises:

> The first premise is that human beings act toward things on the basis of the meanings they have for them... The second premise is that the meaning of such things is derived from, or arises out of, the social interaction that one has with one's fellows. The third premise is that these meanings are handled in, and modified

> through, an interpretive process used by the person in dealing with the things he encounters. (p. 2)

Consequently, the accomplishment of human group life should be viewed as an intersubjective process where people develop meanings about objects by interacting with others. Meanings are therefore social products, "...creations that are formed in and through the defining activities of people as they interact" (Blumer, 1969, p. 5). By viewing human life as group life, where people are in a process of socially constructing meaning about the world of objects in which they live, symbolic interactionism requires that the researcher be attentive to the way in which people convey meaning about objects to others. Accordingly, linguistic interchange and activity within the life-worlds of the "other" become the focus of the symbolic interactionist.

Adopting the pragmatist stance on agency, interactionists emphasize the active role people play in shaping their environments and destinies (Mead, 1934; Blumer, 1969; Prus, 1996, 1997). Rather than treating individual behaviours as a result of external factors causing people to act in one way or another, interactionists stress the human capability of engaging in minded and meaningful behaviour. At the same time, interactionists recognize reality as not only being socially constructed, but also as being obdurate. Blumer (1969) employs the notion of an "obdurate reality" to suggest that human group life takes place within a world of objects that can act back upon the actor and resist definition. These objects are given meaning and are interpreted by actors through their interactions with others and through one's own capacity to think in abstract terms and

develop, reformulate and carry out lines of action. The same object may hold different and multiple meanings for each individual and may, at the same time mean something different at different times and in different contexts for the same individual (Mead, 1934; Blumer, 1969).

Humans also have the capacity to be both a subject and object unto themselves (Mead, 1934; Blumer, 1969). Individuals thus have the ability to take themselves into consideration when formulating lines of action. It is this reflexive capacity and the ability to see oneself in the "generalized other" (i.e., the ability to take a generalized set of attitudes or multiple positions towards oneself into consideration) that an individual develops a conception of self (Mead, 1934; Cooley, 1922). Mead (1934) suggests that individuals formulate the notion of a generalized other during their youth. The generalized other is used as a referent when attempting to anticipate how others may perceive and act towards us. Thus, even without the presence of others, individuals are capable of organizing their thoughts and behaviour around the generalized other – the representation of societal attitudes within the individual (Mead, 1934). As Liebow (1994) states, "Trying to put oneself in the place of the other lies at the heart of the social contract and of social life itself" (1994, p. xv).

Building on the aforementioned premises, Prus (1999) captures the essence of the interactionist perspective in a series of ten assumptions:

1. *Human group life is intersubjective.* Human group life is accomplished (and made meaningful) through community-based, linguistic interchange.

2. *Human group life is knowingly problematical.* It is through symbol-based references that people begin to distinguish (i.e., delineate, designate, and define) realms of "the known" and (later) "the unknown".
3. *Human group life is object-oriented.* Denoting any phenomenon or thing that can be referenced (observed, referred to, indicated, acted toward, or otherwise knowingly experienced), [objects] constitute the contextual and operational essence of the humanly known environment.
4. *Human group life is (multi) perspectival.* As groups of people engage the world on an ongoing basis, they develop viewpoints, conceptual frameworks, or notions of reality that may differ from those of other groups.
5. *Human group life is reflective.* By taking the perspective of the other into account with respect to one's own being that people become objects unto themselves (and act accordingly).
6. *Human group life is sensory/embodied and (knowingly) materialized.* Among the realms of humanly knowing "what is" and "what is not," people develop an awareness of [the material or physical things] that others in the community recognize. This includes attending to some [sensory/body/physiological] essences of human beings (self and other), acknowledging human capacities for stimulation and activity, and recognizing some realms of practical (enacted, embodied) limitation and fragility.
7. *Human group life is activity-based.* Human behaviour (action and interaction) is envisioned as a meaningful, deliberative, formulative (engaging) process; of doing things with respect to [objects].
8. *Human group life is negotiable.* Because human activity frequently involves direct interactions with others, people may anticipate and strive to influence others as well as acknowledge and resist the influences of others.
9. *Human group life is relational.* People do things within group contexts; people act mindfully of, and in conjunction with, their definitions of self and other (i.e., self-other identities).
10. *Human group life is processual.* Human lived experiences (and activities) are viewed in emergent, ongoing, or temporally developed terms.

By delineating the underlying assumptions of interactionist theory, the researcher is better positioned for investigating and understanding the world of the other. Such premises form the theoretical position of this thesis and in turn represent the

sociological lens through which the social world of the hacker has been interpreted.

**Interactionism Online**

In the process of interaction, people use symbols to convey meanings. As verbal symbols, words provide representations for objects, emotions, and behaviours. Non-verbal symbols such as body language are also used to convey meanings about objects. In their methodological discussion on field research, Taylor and Bogdan (1984) suggest that it is necessary for the researcher to be attentive to the "dialogue accessories" that accompany people's verbal symbols. Such things as one's gestures, tone of voice, and speech patterns add additional meaning to what someone says and therefore help in the researcher's interpretation of the meanings of words.

When interacting with other people over the Internet the researcher is presented with a different, somewhat more limited, range of dialogue accessories. However, everyone participating in online discussion must interact within the same boundaries. In entering into this virtual life-world, part of the process of achieving a sense of intimate familiarity with one's subject matter is experiencing the same sorts of ambiguities others encounter when engaging in online activity and communication. Not only are there various forms of communication on the Internet (e.g., e-mail, IRC, web boards) there are also a number of conventions (known as netiquette, which are interpreted in various ways), short hand (e.g.,

emoticons, acronyms) and jargon one learns to follow and interpret.[4] As people spend more time online they tend to develop a greater sense of proficiency with the different ways of communicating with one another.

Although Fine (1987) suggests that the researcher's role is to focus on interaction as it takes place on a face-to-face basis, the Internet allows for sustained interaction, although non-physical, to occur across vast distances. In this computer-mediated, social life-world people with a wide range of backgrounds and interests are spending a significant amount of time forming relationships, developing perspectives, sharing ideas, creating meaningful online identities and virtual objects, and generally, developing and transmitting culture. With a computer and an Internet connection, people can navigate the online realm, moving from one interest to the next as quickly as they move from one online persona to another.

While having to interact through a computer may be seen as an obstacle to effective communication, to certain individuals online interaction removes some of the limitations encountered during face-to-face interaction. For instance, the perceived anonymity one is afforded by the Internet permits those, who may otherwise be too shy, to engage in conversations about things of interest to them. At the same time, one's sense of anonymity may provide for a more open discussion about activities that may be deemed by outsiders as deviant and necessary of some form of sanctioning. From a researcher's standpoint, the

[4] Aspects of online talk are discussed in Chapter 6: Hacker Argot.

interest is in having informants feel as comfortable as possible so that they may discuss all realms of activity, experiences and perspectives (deviant or otherwise) that are of interest to them.

Online interaction demands that the researcher be proficient or develop proficiency in achieving a degree of comfort with this medium of communication. In acquiring this knowledge, one necessarily goes through a number of steps -- a natural history -- of gaining competence in the online realm. Experiencing, recognizing and examining the various stages of this process provides a great deal of insight into one's understanding of how others acquire a sense of online fluency and know how. This in turn may very well be what the researcher is interested in studying.

Given their affinity with computers and the Internet, hackers, likely more than any other computer user, have developed a great deal of online comfort and fluency. In discussing his research on the hacker subculture, Dr. Kall Loper suggests that hackers are likely more at home when communicating online than most users (Chawla, 2001). During my real-time chat sessions with hackers, not only were most able to communicate their thoughts quickly, they were also quite articulate in expressing their ideas and perspectives.

**Conceptualizing Subculture from an Interactionist Perspective**

Throughout the scholarly literature on the concept of subculture one finds that there is variability in how the term is defined and applied. Citing Cohen (1955) and Miller's (1958) research on delinquent youth, Fine (1987) indicates

that some researchers treat subculture as a closed and formal structure devoid of social interaction. The symbolic interactionist stance on this matter is to put interaction front-and-centre in one's research, focusing on communication and activity as it takes place in the here-and-now in order to understand how culture[5] is developed and spread (Blumer, 1969; Fine, 1987; Fine & Kleinman, 1979; Prus, 1996, 1997; Shibutani, 1955). From this point of view, subculture can be defined as, "...a set of interactionally linked people characterized by some sense of distinctiveness (outsider and insider definitions) within the broader community" (Prus, 1997, p. 41). Some of the fundamental conceptual features of subculture identified by interactionists include: (1) an understanding of group culture in terms of the multiplicity of involvements individuals have with various groups; (2) the processual nature of subculture; (3) subcultural variants; and, (4) characteristics which constitute the culture of a subsociety and distinguish individual subcultures.

### *Culture Formation: The Subcultural Mosaic*

While a study may focus on a particular subculture it is important to recognize that the cultural characteristics of any group are formed and influenced by individuals' perspectives as they are developed in other aspects of their lives through an ongoing process of self-reflection and interpretation. To appreciate how subculture is developed, it is necessary to explore individuals'

[5] *Culture* is defined in this thesis as the cumulative body of ideas and practices for a given group of people (Becker, Geer, Hughes & Strauss, 1961).

understandings not only as they are constituted in the activities and interactions of people within particular life-worlds, but also by examining the interpretive process and individuals' perspectives brought to the group from outside or external involvements.

Building upon the works of Blumer (1969) and Strauss (1982, 1984, 1993), Prus (1997) stresses that society is best understood by examining people's multiple involvements in various life-worlds:

> Rather than envision any society or community (from the most elementary and homogeneous human communities to the most complex and diversified societies) as characterized by a dominant or highly pervasive culture, it is posited that any society or community consists of people acting in a mosaic (or set, configuration, amalgamation, matrix, or collage) of diverse subcultures or life-worlds that exist in temporal, dialectic (and in many cases only indirectly connected) relationships to each other. (pp. 36-37)

Prus (1997) argues against treating culture as a homogenous "overarching singularity." He suggests that by doing so we lose sight of how culture is formed between individuals in their various everyday interactions in a series of different settings. Instead, Prus maintains that the cultural aspects of human group-life should be envisioned in terms of a subcultural mosaic: "...the multiplicity of subcultures, life-worlds, or group affiliations that constitute people's involvements in societies or communities at any point in time" (1997, p. 36). Viewed in these terms, culture is very much a humanly enacted phenomenon dependent on individuals interacting and drawing on their knowledge garnered in and from a series of life-worlds or subsocieties.

Most of the research on subcultures has left it unclear as to whether the term refers to a group of people or to a group's shared ideas (Arnold, 1970; Fine & Kleinman, 1979). While "subsociety" is defined in purely structural terms based upon membership in groups or smaller segments of society, the cultural elements (i.e., ideas and practices) that characterize a particular subsociety make up its subculture (Fine & Kleinman, 1979). As people enter into or become part of a subsociety their membership requires that they adopt the group's cultural elements (Fine & Kleinman, 1979). Within each subsociety, cultural understandings are developed and influenced by the perspectives brought from each individual's involvement in and knowledge of other life-worlds. Drawing upon the perspectives of various *reference worlds*,[6] individuals' viewpoints are adapted to the different contexts and situations in which they find themselves (Shibutani, 1955). Therefore, individuals may simultaneously or alternatively identify with more than one subculture (Shibutani, 1955). It is in this way that group-life is said to be *multi-perspectival* (Prus, 1997).

Shibutani (1955) points out that it is possible for anthropologists focusing on isolated societies to adequately discuss "cultural areas" in geographical terms. However, in "modern mass society", rapid transit and mass communication (e.g., the media, telephone, Internet) provide for numerous communication channels. Through these networks individuals are able share and encounter cultural

[6] As Irwin (1970b) indicates, although Shibutani (1955) does not refer to "reference worlds" or "social worlds" as subcultures, this is one of the ways in which the concept can be applied.

knowledge without ever being in close proximity to one another (Fine & Kleinman, 1979; Prus, 1997; Shibutani, 1955). As such, geographical boundaries may inhibit, but not halt, the transmission of culture:

> [S]ince communication networks are no longer coterminous with territorial boundaries, culture areas overlap and have lost their territorial bases...Each social world, then, is a culture area, the boundaries of which are set neither by territory nor by formal group membership but by the limits of effective communication. (Shibutani, 1955, p. 566)

The Internet is a good example of a communication medium through which culture can be developed and conveyed both directly (e.g., one-on-one chats) and indirectly (e.g., information presented on web pages, newsgroups, etc.) to people that might otherwise never "meet." Online access to a wide range of different groups espousing varied cultural understandings permits for the formation of perspectives on a grand scale. Although the Internet creates restrictions for more complete associations (i.e., of the kind one acquires through face-to-face interaction), individuals are able to form perspectives that are identifiable both on- and off-line.

### *The Processual Nature of Subculture*

> *Culture is not a static entity but a continuing process; norms are creatively reaffirmed from day to day in social interaction. (Shibutani, 1955, p. 564)*

If we work from the interactionist premise that group life is processual, and meanings therefore historically relative, it follows then that subcultures are more or less in constant flux. Irwin (1970a) aptly discusses the need for a

processual conceptualization of subculture in discussing the historically and contextually relative nature of meanings:

> In conclusion, a subculture must be analyzed historically. With the concept of subculture that was presented here – as something strongly akin to the concept "culture" which is changing and evolving constantly – to understand the behavior of the subculture participants, the investigator must be cognizant of the time dimension of the phenomenon. Subcultural systems are undergoing constant changes due to internal processes of growth and change, and due to varying circumstance of the greater cultural-social setting of the subculture. Therefore, certain behavior at one point of time does not have the same meaning, and relationship to the subculture as it has at another time. (p. 111)

As individuals enter into different groups and experience others' perspectives, the way in which they think about the world is influenced in some way. Through a process of interchange, the meanings people attribute to the world of objects in which they live may be challenged or confirmed and perhaps, refined (Fine & Kleinman, 1979). As people encounter and dwell on these ideas, their cultural understandings are negotiated both externally and internally through the exchange of verbal and non-verbal symbols and a process of self-reflection.

As Prus (1997) points out, when individuals sustain an enduring intersubjective understanding of the objects that make up their particular life-world(s), they develop more sustained cultures. However, given the pluralistic and information-oriented nature of modern western societies, where individuals are more or less in contact with a number of different cultures, subcultures are likely to fluctuate over time to varying degrees. Some subcultures have undergone totalizing changes in a very short period of time, while others have

changed very little over the centuries. The extent of change would seem to depend on such things as the rules of a given society, encounters with outside ideas, and actions taken to alter others' understandings. Even in more modern societies, where contrasting perspectives are encountered on a continual basis, if individuals are part of a society wherein ideas opposing their own are effectively countered, they too may be able to retain a relatively stable or static subculture.

The changing composition of group membership is a structural aspect of a subsociety that is inevitably fluid. Some groups might continually be accepting new members, whereas others are more closed. However, as time passes individuals seek alternative involvements, age out of groups, and pass-away, therefore necessitating that these groups attract new members or cease to exist. Some groups may be formed for very short periods of time and others may exist forever (even though membership changes). As group membership changes, newcomers bring with them a series of perspectives acquired in other contexts. The possibility of encountering differing viewpoints brought by newcomers has the potential to impact on the existing ideology of a subsociety. Thus, fluidity of membership is a key structural element impacting on the cultural aspects of a society.

Treating culture as "something in the making" (Prus, 1997) has a profound effect on how social scientists study subculture. Rather than treating a subculture as being static, it necessitates that researchers develop an understanding of the ongoing and emergent aspects of culture within particular groups. As Fine and

Kleinman (1979) indicate, however, it is problematic to investigate something that is in flux, as findings will only capture a subset of information across a certain time period. Nonetheless, the fluidity of personnel and information across subcultural boundaries needs to be taken into account (Fine & Kleinman, 1979).

***Subcultural Variants***

Prus (1997) asserts that there are, "...an endless assortment of contexts (and levels) in which the concept subculture may be applied..." (43). The terms *idiosubculture* (Fine, 1987) and *groupculture* (Gordon, 1970) have been used by researchers to distinguish a smaller segment of an overarching subculture, the small group, wherein the group's culture is created and shared amongst individuals who know one another. For these researchers, the term *subculture* is reserved to describe the larger social units through which culture is disseminated, where members may not interact directly with one another, but still share a common culture. Expanding on this idea, Prus (1997) offers a set of working definitions for researchers to apply to the different contexts or levels of a subculture. Of particular interest to this thesis are the distinctions Prus (1997) makes between *transnational* and *local* subcultures.

The hacker subculture is very much what Prus (1997) has termed a "transnational subculture." Transnational subculture is used to define a group that is connected by some focal activity over a broad geographical region (Prus, 1997). Therefore, the focal activity of hackers is hacking and its related activities, and the broad geographical region they cover, via the Internet, is the world. As Prus

(1997) points out, it is not necessary for members of a subculture to ever meet face-to-face during their interactions or even know of each other's existence in order for a subculture to exist:

> While contingent on communication between the participants, subcultural communication is not limited to face-to-face interaction (consider mail, telephone, and computer linkages), nor need it imply direct interaction between all members of the subculture (others may provide interactive linkages). Thus, while a great many subcultures are built directly on face-to-face interactions, it is not necessary that those involved in any particular subculture reside in the same geographic setting or even know of each other's existence. (p. 41)

Each of the different groups that were investigated in this study can be seen as existing, for the most part, autonomously from one another. These groups represent what Prus (1997) has termed "local subcultures", or simply, smaller groups of hackers, although operating somewhat independently from the transnational subculture, very much identify with the larger hacker community.

***Characteristics of Subculture***

In examining various theoretical writings on subculture (e.g., Fine & Kleinman, 1979; McCaghy & Capron, 1997; Prus, 1997; Shibutani, 1955) and other qualitative research directly or indirectly employing the concept (e.g., Becker, 1973; Fine, 1987; Humphreys, 1975; Letkeman, 1973; Mitchell, 1983; Prus & Irini, 1980), a consistent pattern of the common conceptual characteristics

of "subculture" has been observed.[7] A brief overview of each of these characteristics is presented here in terms of working definitions. Although the following characteristics are presented separate from one another, a more complete appreciation of a community's culture is accomplished by envisioning each element as being related to the next and coming together to form an interconnected whole, resulting in the formation of *subculture*:

(1) **Ideology or Perspective** – The way in which a group views and makes sense out of the world that serves to justify the existence of the group and its accompanying values and beliefs;

(2) **Rituals or Routines** – A common set or patterns of activities, which are particular to a subsociety, but more importantly differ from outside understandings in terms of the meanings applied to them by insiders;

(3) **Argot** – A distinct language and way of speaking where new symbols may be developed within the group context and additional meanings placed upon words used by both insiders and outsiders;

(4) **Norms** – Rules of behaviour or expectations of appropriate conduct developed within the group context, which exist both formally and informally as ways of governing members' behaviour;

[7] The idea for presenting subculture in terms of the various characteristics identified here came as result of a lecture by Dr. Dorothy Pawluch (of which I was sitting in on as a teaching assistant). The purpose of the lecture was to introduce "subculture" to an undergraduate sociology of deviance class at McMaster University. Soon after I began exploring the concept further in different interactionists' research and found that, while the terminology differed somewhat from researcher to researcher, the ideas presented by Dr. Pawluch were more or less consistent throughout others' writings.

(5) **Artefacts** – objects (both physical and non-physical) that represent the symbolic items of a particular subsociety as they may be a focal point of group activity and hold special meaning due to their historical or nostalgic significance imputed upon them by insiders;

(6) **Identity** – Definitions of self revolving around how individuals in the group see themselves and how they feel outsiders see them.

In subsequent chapters the concepts of *ideology* and *argot* will be explored more thoroughly and applied directly in analysing the hacker subculture.

# CHAPTER THREE

# METHOD

## ETHNOGRAPHIC INQUIRY

In outlining the methodology of this thesis, I take the stance that it is necessary to make indications of where we, as ethnographers, are coming from when we approach our studies. This involves not only laying out one's theoretical orientation, but also locating oneself in the research and bringing to the fore a recognition that what the field researcher presents is his or her interpretation of the setting and interactions therein. In presenting my own subjective disclosures, I hope to share a small portion of the research experience and, in turn, offer a more complete picture of the study's results.

As Bailey (1996) points out, that which we learn from our setting is affected by who we are, including our personality, status, appearance and expertise. Like any other individual, we too are bound to our interpretations. And while our interpretations are guided by theoretical and methodological principles, we cannot ignore personal factors that influence our research in one way or another. The methodological approach to be described attempts to not only illustrate the procedure, but also make indications as to the types of obstacles and sentiments that arose throughout my time in the field. In giving recognition

to those aspects of the research that affect the process of data collection, I hope to provide a more complete picture of the field research process, a process that while sociologically grounded, remains true to the human aspects of making negotiations, forming relationships, reflecting upon situations, deciding on courses of action, and developing understandings.

### *Interactionism and Ethnography*

Viewing human group life from an interactionist standpoint has profound implications for the type of approach taken to study human behaviour. Blumer (1969) suggests that if one wants to study human behaviour, he or she should take a "naturalistic" approach. Such an approach requires that the researcher make an effort to get inside the world of the people being studied and place him or herself in the position of the individual or the collectivity being investigated (Blumer, 1969). Additionally, Blumer (1969) stresses that the researcher should strive to acquire a body of relevant observations on the group being studied. Therefore, Prus (1997) suggests that an ethnographic approach be adopted to gain "intimate familiarity" with one's subject matter, that is, the world of human experience.

An ethnographic approach allows the researcher to acquire an inside perspective on how people actively engage the world in a meaningful, interactive, and interpretive fashion. Prus (1997) posits that ethnographic research requires that the researcher learn about human lived experience through "interactive inquiry." He states that it is only by venturing into the life-worlds of the other and interacting extensively with those being studied is it possible to fully

appreciate human lived experience. Prus (1997) maintains that the goal of the ethnographic investigator is to examine and analyze human group life "*as it is constituted in practice*" (Prus, 1997, p. 195, emphasis in original). To accomplish this, he suggests that the primary pursuit of the ethnographer is "to achieve a thorough, sensitive, and fine-grained descriptive account of the life-world of the other" (1997, p. 192). While ethnographers may limit themselves to this task, he argues that a second and related objective is to develop analytical concepts that help to establish more precise understandings of the situations they are examining – an objective I attempt to adhere to throughout the analysis.

In order to collect ethnographic data, Prus (1997) suggests that the researcher acquire information about people's lived experiences through observation, participant observation, and interviews. While observational data is limited to making inferences about the meanings that others attribute to objects, participant observation and interviewing allow the researcher to obtain an in-depth understanding of the intersubjective realities that are actively forged within particular settings (Prus, 1997).

***Dealing with Preconceptions***

As an ethnographic study, the research and analysis in this report can be envisioned as exploratory in thrust. It is exploratory in the sense that, although each ethnographer begins with a theoretical and methodological toolset, the

imposition of prior understandings of a particular group are forgone[8] in favour of acquiring an insider perspective and achieving a sense of intimate familiarity with the particular group being investigated. While it is impossible to simply forget one's previous impressions and understandings of a specific group, it is necessary to keep an open mind to meanings people apply to the objects they make reference to within their particular life-worlds.

With that said, what one learns in theory, does not always play out to the same extent in the field. Even with a few years of background research and reading on grounded theory, at the outset of this project I had already faltered on one of the primary rules of ethnographic research – I had developed preconceived notions about the hackers I sought to understand. As Taylor and Bogdan (1984) advocate, the research design should be flexible from the outset as, "...the preconceived image we have of the people we intend to study may be naïve, misleading, or downright false" (p. 16). Perhaps the most fundamental mistake a person can make in this regard, is to apply a pre-formed, moralistic definition to the group under study. However, given the widespread, outsider (media, layman, legal) consensus that hackers were computer criminals, I thought it would be interesting to examine this criminally deviant subculture and see how it worked from the inside.

[8] As mentioned, the degree to which one can set aside his or her personal biases and preconceptions is highly questionable. However, being aware of such things as researcher bias, reactive effects, and related issues allows the researcher to evaluate their own impressions. At the same time, presenting one's subjective interpretations as part of the research process helps to frame the analysis so that others can better understand the researcher's findings.

I ended up meeting with a group of hackers after coming across their web page and seeking permission, via e-mail, to attend one of their meetings. Although the rules laid out on their site suggested that all were welcome, I was sceptical. The following day I received an e-mail reply indicating that I was more than welcome to attend. However, after my first meeting with this group, I was unsure as to whether or not these people were indeed *hackers*. The topics of discussion at the meeting had little to do with the illegal activities I felt were typical of hackers (e.g., creating viruses, stealing passwords, breaking into computer networks). Instead, they discussed the theory behind the Tesla coil,[9] visited the local automotive parts store to sift through an endless array of (what appeared to me) to be useless bits and pieces of electronics, and examined the inner structure of a discarded dial-tone generator (which they dubbed, "The God (Ascension) Box"). In short, nothing of an illegal nature was discussed during the meeting. Instead, what appeared to be of most interest to this group was a desire to find new creative uses for things and an interest in finding out how things work. Even though I had it in my head that I would not pre-judge the group, I found myself questioning whether or not these people were hackers.

I was well aware of how hackers were presented in the media, but there were other social pressures for me to predefine members of the subculture as criminal, and potentially dangerous. For example, before my first meeting with a group of hackers, my father thought it might be prudent for me to take my brother

[9] In very basic terms, a Tesla coil is a device capable of producing an electrical charge that appears similar to a stroke of lightning.

along for "protection." One of my friends, a police officer, joked about staking out the meeting place in case there were any "hostiles." While I was determined not to predefine the hackers I was about to meet, I began to contemplate my parent and friend's notions that this group might be physically dangerous.

There are at least a couple theoretical and methodological observations or lessons I took away from this initial experience of claims-making and labelling. The first insight is theoretical and pertains to interactionist assumptions regarding how people come to understand the world in which they live. As outsiders, my father and friend knew very little of what a hacker was, nor did I. The words of caution and concern that were expressed seem to have had a great deal to do with our lack of understanding and, at times, fear of the unknown. Through linguistic interchange people label and define groups and individuals in order to situate them within their realm of experience and understanding. Such labels carry with them a set of meanings and definitions. Having never met a person such as a hacker before, one relies upon other definitions he or she has come across in an attempt to make sense of how a particular person or group of people may think and act. To my father and friend, the suggestion of me going to meet with hackers, led them to draw upon their notions of what a hacker was. While my friend invoked his police self and accompanying definition of hacker, my father drew upon other second hand knowledge of hackers such as media images and definitions presented to him through previous conversations. Having encountered

similar definitions and having these reinforced by meaningful others put me in a position where I found myself further internalizing their perspectives.

With this in mind, the second, more methods-related observation pertains to one being aware of the relative nature of understanding, and how recognizing that this in itself offers explanatory power when analysing and presenting one's data and findings. It is beyond the field researcher to consciously forget how he or she has previously (and/or personally) defined a group of people. However, what is important is that ethnographers be cognisant of this fact and always be working towards an understanding of a particular group that is not only based upon insider information, but also contemplative of the relative nature of meanings people apply to the world of objects in which they live. Thus, it would seem that a more complete sociological understanding of a particular group of people is offered when the researcher works towards presenting and comparing both insider and outsider definitions.[10]

### *Locating Informants and Deciding Upon the Research Setting*

In order to gain insight into the experiences of hackers, it was necessary to determine the various methods of communication they use and discover where this group tends to congregate. As one might expect, being a fairly geographically disparate group, and given the highly technical (and sometimes

[10] While the terms insider and outsider have been presented here in rather simplistic terms, they serve to denote and contrast the degree to which one can relate (in terms of viewpoints, identity, activity, language, etc.) to a particular group. However, rather than thinking of "insider" and "outsider" in dialectical or contrasting terms it is likely more informative to view them as being on a continuum, with people experiencing a greater or lesser degree of "insiderness" at certain times and places than others.

illegal or covert) nature of their activities, hackers use the Internet (and Bulletin Board Systems to a lesser extent)[11] to communicate with one another. The Internet represents the predominant medium of choice through which they not only correspond with one another, but also gather as a virtual community.

While "traditional" ethnographic ventures have grounded their inquiries into human behaviour as it occurs in the real world, the Internet has opened up new avenues of communication and has allowed for the formation of virtual communities (Ferguson, 1999; Kleinknecht, 2000; Rheingold, 1993). Therefore, in order to fully appreciate the experiences of hackers, it is not only necessary to meet with them on a face-to-face basis, it is also essential to delve into their communities as they exist in the virtual realm. Working from this perspective, I approached the study by examining hacker interaction as it occurs both on and off the Internet.

Hacker meetings in public settings such as a coffee house and food court were the primary offline settings in which data were collected. My first meeting with a group of hackers took place at a popular coffee shop. As I noted before this meeting, "It seemed kind of interesting to me that a group that is stereotypically known as being anti-social and involved in illegal activities would choose [a popular coffee shop] as a place to meet" (field notes). However, my

[11] A Bulletin Board System (BBS) is a computer that people can dial into using their modem. Those people who have access to the BBS can: copy files to it from their own computer; copy files from it to their own computer; send messages to other users of the bulletin board; and, play multi-player games. BBSs are still around in abundance but have generally been superseded by the Internet.

first experience with a group of hackers quickly reinforced that it would be necessary to set aside any such preconceptions and open my mind to the *new* reality I was encountering.

At the outset of the project it was difficult to find a group of hackers geographically close enough to be accessible. However, after a series of searches on the Internet I came across a web site that provided information on (offline) hacker meetings that had been held on a monthly basis for a number of years in cities across Canada and around the world. Initially, it was necessary to drive a few hours to meet with one of these groups. However, this initial meeting generated a series of contacts and suggestions of people to talk to and places to visit on the Internet to learn more about their subculture. The first group that I had met with started with approximately five to eight members, but over the course of the year had grown to as many as twenty people. When I first attended, the group was still in its infancy, having only been officially in operation for about five months. This provided for a unique perspective in terms of how people became involved, solicited membership, conveyed initial perspectives and engaged in preliminary group identity work. Over the course of the first year I attended monthly meetings with this group and continued correspondence with members of the group via the Internet for the entirety of the study.

Upon setting out to my initial meeting with this group, I encountered some of the inconveniences endured by ethnographers during the course of data collection:

> I was late for the meeting, which began at 7 p.m. On my way there I faced heavy traffic, ran into three accidents, and got lost three times before actually making it to my destination. I arrived at 8 p.m. and once I got there I headed directly for the washroom. (field notes)

At this time I had also been arranging to meet with a second group of hackers at one of their meetings. My meeting with this group had been coordinated in advance and was to occur exactly a month after I had met with the first group. However, this did not quite work out as planned:

> I was supposed to meet with [the second] group tonight, however when I got to the meeting place there was no one there. The food court... was to be where the group was congregating. Today, when I asked my dad for directions to the [location] he told me it no longer existed and that it had been replaced by [a different building], but he was pretty sure there was still a food court there. On the [the group's] web page it said that they meet at the food court on the upper-level of the [building] from 6 to 8 p.m. the first Friday of every month. A couple days earlier I had confirmed with [the meeting organizer] that they were still meeting on this date, and he told me they were. Perhaps it could be that they decided to change locations and/or time without updating their meeting information on their website. Or they may have cancelled the meeting without informing me. Or maybe they wanted to lead me on a wild goose chase... (field notes)

It turned out that they did meet that night, but only a few people were going to be around, so they got together at a different location. In choosing to come to this meeting, I had made the choice to forgo my meeting with the first group (as it was also their night to meet). I also missed attending my brother's high school convocation (which I had unfortunately justified on the need for data collection).

In building the research relationship with informants, each party (i.e., the researcher and the subjects) must necessarily place a significant amount of trust in

one another. In this case I had trusted that the meeting would be where it was supposed to be or that I would be informed otherwise. This was not a serious breach in the trust relationship, but one that nonetheless caused me a certain degree of inconvenience. In order to ensure continued communication with this group, I bit my lip and remained congenial when following up with them. Experiences such as these did not make me lose faith in the research. I simply wrote them off as learning experiences and moved on. While there were some setbacks encountered and sacrifices that needed to be made during the course of the research, the experience was overwhelming positive and very rewarding in terms of data collection and field research practice.

About a year into the project a new monthly meeting had been initiated closer to where I was living and thus made it easier for me to attend meetings. This group was somewhat different in its membership composition (e.g., more university students) than the first group and slightly larger with approximately twenty members. In addition to meeting with the group offline, I spent a number of hours interacting with members via the Internet in their Internet Relay Chat (IRC)[12] channel. The group had established its own IRC server, which meant that they had physical access to the computer that ran the IRC server program and

[12] IRC will be discussed more extensively later in this chapter, but for the time being it seems pertinent to provide a brief description. Internet Relay Chat (IRC) is a vast multi-user discussion forum that allows users to communicate textually in real-time (i.e., chat) over the Internet. Each IRC server (e.g., DALnet, EFnet) hosts hundreds of channels devoted to various topics (e.g., hacking, pop music, fast cars, football, stamp collecting). Individuals can also set up their own private IRC servers, which others can connect via the Internet.

therefore, could ultimately control as much of the channel's discussion as they liked.

A third meeting developed in a nearby city about nine months into my research. Like the previous group, this group also established its own IRC server and channel. While I never met with this group face-to-face, I did interact with and interview some of its members over IRC.

The final group I met with was constituted by those with an interest in the annual Defcon hacker conference that takes place in Las Vegas.[13] I acted as a participant observer in the group's IRC discussions and as I began to get to "know" members of the channel, I started to solicit interviews. Most were more than willing to be involved, but some were unable to or hesitant, for a number of different reasons (e.g., time limitations, distrust of the project).

I met other informants through hacker discussion forums or based on referrals from the people I had been meeting. I also attempted to contact various hacker "icons" – i.e., hackers that had gained status within circles of the hacker community as a result of such things as their computer knowledge and programming skills, significant media attention and hosting of popular web sites. My requests for interviews with these individuals were not met with much interest, mainly due to self-reported time restrictions. Towards the beginning of the project I posted a message to a hacker newsgroup asking for their input into

[13] Attracting over 4,200 attendees in 2001, Defcon is the largest hacker conference in the world and has been in existence since 1993. The conference is geared towards those with an interest in computer security. As such, a three-day schedule of events and presentations are planned around this theme.

my study. This effort turned out not to be as valuable as I had first anticipated. While I was e-mailed a couple of references by members of the forum, most replies were more derogatory than helpful (e.g., one response read: "would you like some fries with that education"). Even so, these responses did offer some insight into how uninitiated outsiders were treated in hacker newsgroups.

### *Negotiating Presence and Self-presentation in the Field*

Although Becker and Geer (1970) emphasize the benefits of participant observation over interviewing, they advocate a multi-method approach, including both of these techniques, in order to collect the richest set of data possible. Research solely based on interview data places investigators in a position where they must infer actual events and understandings of particular life-worlds that they have not observed. Participant observation allows the researcher to acquire a great deal of experiential data by observing group activities, interactions, and shared understandings as they are enacted and conveyed in their natural settings. In such settings, subjects are constrained by their real-life situations to behave as they usually would (Becker, 1970). So long as the researcher is not viewed as a threat, subjects will tend to behave as they would if the researcher were not present (Becker, 1970). This last point was necessarily one of serious consideration for my research.

A consistent theme noticed in both interviews and participant observation with hackers was their suspicion of outsiders. On one occasion I was jokingly referred to as an undercover parole officer, on others a Fed and a NARC. Huss

(1998) relates a similar experience in discussing his master's research. He states that he was questioned on many occasions about which law enforcement agency he belonged to. He also points out that, "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" (p. 28).

In the process of gaining acceptance within the subculture it was necessary to make ongoing confirmations as to the legitimacy of my research and constantly negotiate my presence with gatekeepers and interviewees. The following quotes demonstrate the types of bargains and assurances that were made:

> <Dan> Well, it's hard to get people to take you seriously. We, as a community, have been burned way too many times.
> <Steve> By reporters? Researchers?
> <Dan> Yeah, misrepresented to make things sound interesting
> <Steve> I try to tell it like it is. I really try to do my best to let the people I speak to define the paper. I use as many quotes as I can and try to keep them in context. I plan to have a fairly long section on definition. Insider definitions (which vary) and outsider definitions.
> <Dan> Sounds kool, I'd definitely like to read it when it's done. (interview)

Also:

> <Andy> I also want to make sure I can decline to answer a question, if I think it will reveal too much personal or confidential information
> <Steve> Yes, definitely. If I ask ANY questions you don't want to answer, just tell me "no comment" or "next question". I do ask stuff about background, which, of course, you don't have to answer. You can tell anything you like. The hope though is that I will get honest answers :) I am trying to represent the hacker culture in my thesis using responses from people such as your self. Thus, I count on participants not to be misleading. Soooo... are

> you interested? You can quit the interview at any time. Please be courteous though :)
> <Andy> Yeah, I can do that. (interview)

And,

> <Steve> Only a few more questions... I very much appreciate your help with this.
> <Rick> No problem, my pleasure. So long as I get a copy once it's done, heh. (interview)

As the following quote indicates, sometimes it was not possible to convince others of the authenticity of my research:

> <Shane> Ok, here's the deal... I won't be able to participate... Apparently there are people out there pretending to be students working on research papers talking to people with sensitive information. Sorry dude. (field notes)

When it is not possible to establish a sense of trust between the researcher and the informant it is best that one of the parties makes this clear upfront. Otherwise, the credibility of such data is obviously brought into question.

As Burgess (1991) notes, experiences of having to continuously negotiate one's presence within a particular subculture are quite typical in qualitative research. The context changes, new decision-makers are introduced, deadlines re-worked, and reassurances of anonymity and confidentiality made. Nonetheless, the question of how much of a reactive effect my presence was having on hackers "natural" behaviour weighed heavily on my mind. Given their possible distrust of me as an outsider, a significant amount of effort went into ensuring informants of my sincere interest in understanding the hacker world through their eyes. Throughout the research I tried to gauge how well my approach was working. On

this note, I can say that my acceptance and trustworthiness within the subculture was confirmed in a number of ways. Indicators included offers to accompany informants on their trips to hacker conferences, invitations to social events, requests for future appearances at meetings, demonstrations of activities of interest to informants, and frank and upfront personal comments during interviews.

While there are ongoing debates as to the degree of obtrusiveness one should permit in his or her naturalistic studies (and, in fact, how much we are ultimately aware of),[14] I worked from the initial stance of avoiding, as much as possible, any outsider influence that I might inadvertently impose. With that said, it is difficult to evaluate the interpretations others may have us (as researchers or otherwise) without actively seeking these answers. Unless the impact of our presence becomes an element of the study, this effect would be quite difficult to ascertain. Thus, I contented myself with incorporating tactics that I felt would impose the least amount of obtrusiveness while taking into consideration my personal requirements of comfort and ethical commitment.

The question of overt versus covert investigation also arose at the outset of the research. Applying, I presume, a mainstream understanding of hackers, it was suggested to me that, because of the deviant (criminal) nature of hacker activities,

[14] In his Comments on "Secret Observation", Julius Roth (1970) presents a concise, yet insightful commentary on the field researcher's tendency to over-simplify issues of secret versus non-secret research. In so doing, he suggests that neither party – i.e., the researcher and the subjects – is fully aware of all the aspects of the research. Therefore, it is difficult to completely assess the impact a researcher's presence may have on subjects' interpretations. Even when a full explanation of the project has been delivered to the subjects, Roth correctly argues that the subjects will not see the research in the same way as the investigator does.

it would be difficult to achieve a sense of trust and rapport with hackers if they were to know that I was a sociologist investigating their particular way of life. This line of reasoning had to be weighed against my own personal reservations concerning an intentional lack of truthfulness; my initial (perceived) ineptitude in engaging in the same level of technical conversation as hackers; and, ethical obligations to be forthcoming about the research. There was also the alternative argument that, through sincerity I would be able to foster a greater sense of rapport with the group than what could be achieved otherwise. Additionally, as Rosalie Wax (1971) argues, attempts to maintain a fraudulent presence in the field can distract us from our focus of remaining attentive to informants and engaging in self-dialogue when formulating preliminary and ongoing insights:

> In many cases, the finest insights of the fieldworker are developed from interaction within the self... This interaction is constricted and distorted when the researcher is preoccupied with sustaining a fraudulent presence. (Wax, 1971, p. 52)

I decided that a straightforward, upfront approach with informants would best suit my interests. The same strategy was and continues to be used by Dr. Kall Loper, Associate Professor of Criminal Justice at California State University Sacramento, in his qualitative research on hackers. Dr. Loper indicates that being open with his informants has helped him to win their trust, "...I'm not shy about telling [hackers] who I am and what I do. I give out my business card... When they knew where I stood, they had no problem with me" (California State University, 2003). As the following quote demonstrates, the degree of openness I

expressed when discussing my research turned out to be quite valuable in establishing trust and rapport:

> <Kris> Meetings are open to everyone and you will receive a warm welcome. We've chased off 3 folks over the 10 years we've been doing this, and all 3 were bad for the group as a whole (one undercover reporter, one undercover cop, one flat out blatant criminal).
> <Steve> That was actually one of the things that had to be considered when I started this research: covert or overt observation.
> <Kris> Ya, we appreciate it when folks are up front with us... journalists, reporters, cops, feds, etc, are all welcome... just tell us who you are first.
> <Steve> That's good to hear... (interview)

Before ever physically entering into the field I carefully considered how I would go about making my initial face-to-face presentation. Questions such as how to dress, what to say, what to look for, and what to bring seemed of importance, not only in terms of collecting data, but also in how I would actively control first impressions. I decided that, although I would, for the most part, be seen as a researcher, I would attempt to minimize the negative reaction the group might have towards an outsider in this role. The particular strategy I employed was that of blending in.

Blending in was accomplished in a number of ways through how I chose to present myself. First, given what I knew of the setting in which we would be gathering (i.e., a popular coffee house) and other factors such as the predicted age and social class of the group, I decided upon a particular style of dress. Having read on hacker web pages about the predominance of black clothing in their culture, I figured that my casual, grey and black shirt and pants, without any

particular branding or flashy design, would be a fair bet as to not attract a significant amount of attention. Pens, paper and tape-recorder were left behind as I felt that such items might reinforce my identity as a researcher (and outsider).[15] The effort taken to blend in, in no way had to do with any attempt to deceive the people I was meeting with. Rather, I took this approach to reach a certain level of comfort in fitting in and to avoid any sort of distraction my incongruent appearance might bring. In fact, although measures were taken to fit in by adapting my physical presentation, I had decided from the outset I would be completely forthcoming about my role as a researcher. In stating my interests, a certain amount of comfort surrounding my feelings of fitting in were exchanged for the comfort in knowing that I was being as honest and upfront as possible. I introduced myself to others sometimes on a person-by-person basis and at other times, when in a group setting, as a general announcement. The same tactic was used in meeting people both online and offline.

During initial meetings, I tended to keep questions to a minimum and when I did raise them, I tried to stay within the general theme of the discussion, which helped me to remain non-disruptive. Aspects of the culture and various activities and perspectives were constant themes of discussion, and therefore it was easy to engage in these types of conversations. Even when topics required

[15] However, I did note after my initial meetings that pens and papers were commonplace during these gatherings as people in the groups I met with use the material to jot down diagrams, reference material, names, phone numbers, etc. Thus, I began to bring a folder with a pen and paper in case anything did come up during the meetings that would be of interest to the study. This simultaneously allowed me to fit in better with the group. In addition, I kept a voice-activated tape-recorder in my car in case the opportunity arose to do an interview and also to record a verbal transcript of the meeting during my ride home.

more insider knowledge to participate in the discussion (e.g., when highly technical terms or jargon were used), I found that as long as I showed a general interest in what was going on and took a moment to contemplate what was being said, most, if not all of my questions were welcomed and time was taken to answer them (both for me and others in the group who might not understand things). The actual composition of these groups tended to work out to my advantage. Both "newbie"[16] and elite hackers alike tended to be represented during the meetings. As these assemblies were open to anyone with an interest in hacking, questions and their accompanying explanations were expected.

Attempts to remain non-disruptive became more trying when opinions were offered that conflicted with my own values. I did my best to keep personal perspectives to myself so as to avoid influencing the natural interactions that were occurring between people. As the following field note excerpt reveals, this was difficult to do at times:

> There seemed to be a lot of hatred in the group, especially expressed by John and Ryan, not towards people, but rather towards companies and big business. For example, John said, "I'm not interested in hurting people. I would prefer to blow-up billboards."... I found that it was hard to hold myself back from some of the discussion they were getting into, especially when John was talking about blowing up billboards. (field notes)

By not coming across as antagonistic, I believe I was able to appear as either neutral or sympathetic to their ideas. This in turn helped to develop a social atmosphere in which informants felt comfortable about disclosing those things

[16] In the context of hacking, "newbie" is a term, often used in a derogatory way, to label the inexperienced or uninitiated hacker.

that were of interest to them. As Fetterman (1991) points out, a non-threatening and unobtrusive demeanour can help to build relationships within the field and thus facilitate the research process. Understanding that the activities engaged in and the perspectives promoted are not our own, but those of the group we are trying to understand, and recognizing that our role as researcher is that of being student and not moral crusader, it becomes easier to avoid expressing confrontational viewpoints. Internalizing and accepting this role allows the researcher to focus on the primary goal of ethnographic research: understanding the viewpoints of others from their perspective.

Whenever questioned about my presence and the purpose of the study, I focused on the objectives of learning from hackers about hackers, that I was interested in their viewpoints, what they liked to do and that I would be non-judgemental about anything they might say, think or do. More so, I tried to back this up by being attentive, constantly interested, and, as mentioned, keeping oppositional comments to myself or avoid saying anything I thought might influence the group in one way or another. During my first meeting, I attempted to say very little and sat back and listened as I felt that this strategy would allow me to focus on what was being said and help me to appear non-confrontational.[17] In doing so, it should be noted that, while we may not verbally say a lot during

[17] Taylor and Bogdan (1984) suggest that the investigator remains unobtrusive and relatively passive to help put subjects at ease, dispel notions of obtrusive research approaches, establish an identity as an "okay" person, and learn how to conduct oneself appropriately in the setting. While this strategy is important to keep in mind throughout the entirety of one's research, it's particularly important at the outset of a project as initial interpretations are being formed on both sides.

our initial encounters with individuals, the absence of verbal communication, as well as the non-verbal symbols we unintentionally transmit, send a series of impressions to others. By saying nothing, we are likely communicating a great deal of information we may or may not be aware of.

As the research progressed, I began to find that my identity as a researcher might have actually been beneficial in terms of developing rapport, establishing legitimacy, and maintaining relations within the subculture. Even before my first time meeting with a group of hackers, one hacker expressed that he appreciated having someone in the academic community take an interest their way of life:

> Steven...
>
> I hope my reply doesn't come too late, because your attendance would be welcome and appreciated. Our meetings are in their infancy, and we encourage everyone to come out and check them out without fear of being judged or ridiculed...
>
> We appreciate your e-mail and your interest in our meetings (and in the hacker culture at large, if I may speak for more than just myself ;) is encouraging to say the least.
>
> Don't hesitate to get back to us with any further questions -- we look forward to seeing you on the sixth! (e-mail correspondence)

As an ethnographic researcher, the ultimate goal is that of acquiring an insider understanding of the social life-worlds being explored. This sort of understanding is only achieved by devoting one's full attention to learning and seeing things as the people being studied see them. Fetterman (1991) reiterates this point, "A lifelong commitment to learning is essential to grasp the inner workings of any group. A field-worker must be willing to be a student, taught by

the individuals under study" (p. 88). By striving for this sense of deeper understanding and engaging in the various tactics necessary to do so (e.g., attentiveness to those being studied, keeping an open-mind, resolving points of misunderstanding), one will only be held in greater esteem by the people he or she is investigating. This emphasis on learning held particular salience during my investigation. The mutual goals of learning, understanding and knowledge very much fall in line with the principle characteristic of the hacker perspective – i.e., an intense drive to understand things at a base level. Therefore, rather than being seen entirely as an outsider or a potential threat to their way of life, my status as a researcher helped in achieving acceptance and respect resulting in a strengthened sense of "insiderness" and rapport with the people I was learning from:

> <Steve> What would you say characterizes a hacker? Is there a hacker identity?
> <Mathew> That depends on who you talk to. The thing that I use to judge people is their Quest for Learning. Are they doing this to learn something, or are they just looking for attention? Take yourself for example - you're a hacker. You want to know. You don't mind asking, and you don't seem to be starved for attention.
> <Steve> Interesting... I never thought of it that way. (interview)

I not only took this comment as a compliment, but also as a marker of the success I had been having in developing trust and rapport.

As Shaffir and Stebbins (1991) point out, field researchers, through their ongoing direct interactions with subjects, have a significant advantage over other more quantitatively oriented methods. This advantage is that of the subjects' respect for the researcher as being sincerely interested in their activities, experiences and viewpoints: "For here is a scientist who is viewed by group

members as interested enough in them and their activities to maintain extensive direct contact instead of relying solely or chiefly on such substitutes as questionnaires and measurement scales" (Shaffir & Stebbins, 1991, p. 20). When the researcher is able to achieve this level of respect amongst subjects, they tend to reciprocate by sharing their time and perspectives. An in-depth interview that permits subjects to talk about things that matter to them can be quite rewarding to both the researcher and the subject (Berg, 2001). Berg (2001) likens a well-developed long interview to reading a good book: "Even after several hours, there is often a feeling that only minutes have passed" (p. 81). So it is with qualitative research when the spotlight is placed clearly on the subject – "the star of the show."

If rapport has been properly established and time permits I believe other ethnographers will have similar experiences as I had in researching hackers. Subjects will spend hours showing you their favourite gadgets, telling you how they got them, why they like them so much and what they mean to them. They will tell you what got them interested in what they do, what they really like or do not like about themselves and others in the subculture, what it means to be a member of the group, and how they make their decisions and justify their behaviour. They will invite you to their meetings and conferences and into their homes to do interviews and share in the group's interactions. Achieving this level of rapport is the closest a researcher may ever come to looking behind the masks of frontstage appearances and acquire a glimpse of their subjects' backstage

selves. Through sustained interactions with subjects, the researcher's scholastic rewards are that of gaining insight into the life-world of others, achieving sympathetic introspection and acquiring intimate familiarity with the people one seeks to understand. As Mike states, people respond positively towards others who respect their humanness, not only in research, but also in everyday life:

> <Mike> In my opinion asking someone how something is done, etc is one of the biggest compliments you can pay that person... For me, personally, it all comes down to respect and as you put it, rapport. Because we're all people first right? If you appeal to a person's basic needs as a person then the rest is gravy. (interview)

There is much to be said for an approach that recognizes the fundamental human qualities of wanting to share ideas, experiences and perspectives and ultimately, be understood.

### *Collecting Data Online*

Aside from the offline meetings and the interviews I conducted, numerous hours were devoted to observing and sometimes participating in hacker conversations in Internet Relay Chat (IRC), scouring over numerous posts to hacker newsgroups, sifting through hackers' web sites, and reading over documents (e.g., online magazine articles, "how-to hack" manuals, writings describing the subculture) they offered for download.

Internet Relay Chat tended to be the main way in which I met and interacted with hackers online so I will take a moment to give a general overview of this communication medium. IRC is a text-based, multi-user online discussion forum. By running an IRC software program on his or her computer, an

individual can engage thousands of different users in "real-time", text-based chat. IRC is laid out in terms of channels[18], with each channel catering to a different area of discussion. Numerous people can join a channel at any given time to participate in or observe the discussion. As well, each IRC user can create his or her own channel, which other users can join. To indicate topics of discussion in a particular channel, each channel is given a name such as #hacker, #cars, #party, etc. When a person enters the channel there are usually a number of other individuals in the chat session at the same time. In the IRC program I was using (mIRC), each person's name (a pseudonym chosen by the individual) appears along the right hand side of the screen. When a person "says" something (i.e., types a message) in IRC their message appears on the left hand side of the screen for everyone in the channel to read. Each new message appears below the previous one. To give you a sense of how this might look, the following is an excerpt from my IRC log file:

<Don> you should see this laptop i've got sitting here
<Don> the screen is totalled
<Andrew> i could imagine
<Don> the inverter is on my desk
<Shawn> ive got an lcd sitting right here in my basement
<Don> the case that holds the monitor
<Shawn> im sure you could find a way to jimmy them together
<Don> is all cracked up
<Andrew> i'll take all the parts
<Shawn> no one said they were free
<Shawn> but chea
<Shawn> p
<Shawn> very cheap

[18] Sometimes channels are referred to as rooms to denote the real-life feeling of meeting in a physical space such as a living room or classroom.

(field notes)

Sometimes a number of conversations occur at the same time and other times a channel may be completely "quiet." To help those whom I had already met offline identify me while online, I simply used the name "stevek" or "steve" while in IRC. Although I chose to use my real name, most people choose a new name (usually referred to as a handle, nickname or alias) to represent themselves online.

In terms of soliciting interviews, towards the end of each offline hacker meeting, I made a point of trying to set up a time to conduct an interview with anyone who was interested. While online, I typically would send a private IRC message to the person I was interested in talking with. If the person expressed interest, I would send them an e-mail outlining the project. Along with the e-mail, I attached a copy of the consent form, which they were asked to read over carefully. If we had not met to fill out the consent form offline, the person could e-mail me back indicating that he or she agreed to participate in the study. People were asked to do so either by stating their consent in the e-mail or by adding their name electronically to the consent form. As part of the agreement, none of the respondents' real names or online pseudonyms will be used in this report.

Over the course of the project, fifteen semi-structured interviews were conducted. Each interview lasted anywhere from two to six hours. While most questions in the interview arose on the spot and were guided more or less by the flow of the conversation, I had developed a set of questions shortly into the study, which I refined a number of times during the course of the research and used in

my interviews. By providing some structure to the interviews, I was able to ensure a comparison of particular processes across the experiences of all the respondents. Once the interviews were complete, I began sorting the data (e.g., interviews, IRC chat sessions, e-mail correspondence, field notes from meetings, newsgroup material) I had collected. Given that all of my data had been saved in electronic format, to help facilitate the coding process, I thought I would try my hand at using a qualitative analysis software program. However, of the three different programs I tried, I found them all to be somewhat rigid in one respect or another, so I developed my own coding program (a "cut and paste" macro) in Microsoft Word. In total, 81 different codes were applied and broken down into 10 broad categories (see Appendix A), yielding some 300 pages of coded output. Some of the data were not exclusive to one particular code and therefore, were grouped under a few different categories.

## DISCUSSION

By combining participant observation and interviewing to collect data, I was able to develop a more complete sense of how hackers were interacting with one another and appreciate how certain perspectives were developed and enacted. Questions of a more personal nature or those questions that were better suited for a one-on-one discussion could be raised during interviews and private talks. At other times, it was important that I was there to experience events, so as to not only capture how people interpreted and reacted to specific occurrences, but also to act as an informed researcher when the event was discussed at later times. By

being able to witness things as they happened I was able to better appreciate how participants interpreted situations and, at times, confirm or discredit interview accounts. Additionally, I was able to follow-up people's individual explanations in the actual setting in which they were engaging in the types of things being discussed in the interviews. A set of working hypotheses or hunches could also be followed over the course of the data collection and examined at various points while in the field and during interviews.

Furthermore, by being present during their everyday interactions, I was able to demonstrate a genuine interest in learning about the hacker subculture. This in turn helped in developing the type of rapport necessary to engage hackers in open and upfront interviews and discussions that would help me to better understand their experiences and perspectives.

These first three chapters have laid the groundwork for the results that follow. In introducing the thesis, the first chapter examined the various studies that have been conducted on how the term "hacker" has been socially constructed in popular discourse. Others' findings indicate that hackers have largely been defined within the media as deviant, computer criminals. This represents a significant definitional shift away from the original use of the term, which carried with it positive connotations of technical genius, skill and intelligence. As the majority of research has largely focused upon media portrayals of the hacker subculture it was argued that an interactionist orientation be used to more closely

examine the ways in which hackers define their subculture. In adopting an interactionist stance and an accompanying ethnographic approach, it was maintained that the researcher is able to acquire a more complete analysis of the subculture, which remains true to the experiences of those being studied.

Each of the chapters thus far has emphasized the general thrust of the thesis: to provide a fine-grained overview and analysis of how hackers define their subculture. In working towards this goal, the next three chapters examine how insiders define the term hacker, the key principles of the hacker ideology and the distinguishing characteristics of the hacker language.

# CHAPTER FOUR

# TOWARDS A DEFINITION OF HACKER: HACKER AS A CONTESTED TERM

The very first line of this thesis asked, "What is a hacker?" While there have been various images of the hacker presented in the media, this chapter goes to hackers themselves to offer a description of "what" a hacker is. As Letkemann (1973) suggests, in order to appreciate the perspective of those we attempt to understand, it is essential that we avoid imposing outside order upon the data. Instead, we should seek to "find and analyse the categories that are meaningful to the participants" and look to them to find answers regarding the meaning of their actions (Letkemann, 1973, p. 9). In keeping with this recommendation, this chapter works towards a definition of "hacker" by examining and delineating insider and outsider conceptions of the term. As one of my informants indicates, given the complexity and heterogeneity of the hacker community, actually situating the hacker subculture may prove to be quite a difficult task:

> <Terry> [O]ne can't really say that there's a "hacker culture". To do so is to belittle the individuality of its members -- it's like saying "carpenter culture" or "lawyer culture". The "hacker culture" is wide, diverse, and contains as disparate a bunch of people as you could ever hope to meet... Never to my knowledge has the entire "hacker culture" as a whole -- that is, everyone who called themselves a hacker and fit the general definition -- united in one common goal or ideal. Certainly, large groups of hackers get together and collaborate all the time (Linux development, for example), but there's just as many who believe that Linux is a

> waste of time and disk space. To each his own. (e-mail correspondence)

As I set out on this project, I began to correspond with a researcher from Israel who was in the process of writing her dissertation on the hacker subculture. She described to me the difficulty that one faces when coming up with a definition of "hacker":

> <Orly> About defining hackers - this is a problem, since there isn't any consensus about the definition. There are a number of different names given to the phenomenon and there are differences between elite hackers and lamers, script kiddies, etc. (e-mail correspondence)

As is illustrated by this statement and the following comments made by one of my informants, a number of different people within the "information underground" have adopted the term "hacker" as a label to describe their activities:

> <Terry> "Hacker" can mean anything, from AT&T Switch Ninja to Linux Perl Scripter. It just implies a certain grade of above-average skill and enthusiasm, and unorthodox technique... (e-mail correspondence)

"Hacker" is quite a complicated term to situate, as it is highly dependent upon individual and group definitions. As discussed in the introduction, the term not only varies in meaning from group to group, insider and outsider definitions also tend to be divergent.

By way of the formal labelling process, law enforcement, through the media, has perpetuated the notion of hackers as criminal deviants. The Royal Canadian Mounted Police (RCMP), for instance, offers the following definition of "hacker":

> A hacker is defined by the RCMP as any individual who, via a modem or some other computer-related communication device, can break a computer's code or password and enter the system...These criminals include everyone from petty computer vandals to the top echelons of organized crime. Once inside, hackers can do everything from steal data and sabotage information to simply browse around. (Churchill, 2000)

Some media or mainstream accounts present a more balanced picture of hackers (e.g., Platt, 1997; Sterling, 1992). But, as a number of researchers have found, hackers are primarily defined by outsiders as computer criminals (Arbaugh, 1999; Chandler, 1998; Copes & Huss, 1999; Duff & Gardiner, 1998; Huss, 1998; Jordan & Taylor, 1998; Taylor, 2001). While this may be the case, even some of these studies work from a definition of hackers as criminals and hacking as an illegal activity. For instance, while Jordan and Taylor (1998) argue against pathologizing hackers, they define hackers as "illicit computer intruders" and hacking as "unauthorized computer intrusion" (p. 757). In discussing whether or not hacking can be captured under the rubric of white-collar crime, Duff & Gardiner (1998) refer to hacking as "unauthorized access... which may involve browsing through information held on a computer system" (p. 214). Other social scientists define hackers as "those who invade the privacy of someone else's computer" (Hollinger, 1998, p. 199) and "trespassers" (Rosoff et al., 1998, p. 402). While certain individuals within the hacker community have adopted a similar definition and "recognize" their activities as illegal, hackers, for the most part, argue against external attributions that characterize them as deviant or

criminal. A good example of this can be seen in how hackers describe media portrayals of their activities.

## HACKERS VS. THE MEDIA: CHALLENGING MEDIA DEFINITIONS OF "HACKER"

Hackers commonly and sometimes vociferously attack media portrayals of their activities. Media accounts are often seen as inaccurate, as all hackers are regularly lumped together under a single definition:

> <Ryan> The media usually gives the audience a perception of hackers as being completely malicious, reckless, and a danger to society.
> <Steve> Is that true in any sense?
> <Ryan> Well, the problem with the media's interpretation is that it generalizes the whole culture as one entity. We're not all bad, malicious, and reckless. Many hackers out there are not malicious at all. But because of the media, and the reckless few, we've been labelled as a group. (interview)

Blame is placed on the media for spreading stereotypes and myths about hackers by inaccurately attributing the exploits of computer criminals to hackers:

> <Brandon> [The media] portrays all hackers as this one group of people, which is not true. They say you're a hacker so you're a criminal, which isn't a fact. A lot of hackers are people that work in software companies and develop software and this kind of thing. (interview)

Some hackers indicate that the media should not take all the blame for perpetuating incorrect understandings. The hacker in the following interview excerpt maintains that members of the public, who acquire their understandings of the world through the media, are all too trusting of what they read:

> <Steve> What's your perception on the media's portrayal of hackers?

> <Mike> Well, it's highly ignorant. But also my opinion of the media in general is ignorance. They mostly are in it to sell hype. But it's a twofold issue. On the one side there is the media - who IMO [In My Opinion] *SHOULD* know better and be more responsible, but on the other side there are the people who believe what they're told simply because of where it comes from. It's back to that "if its in print it must be true" thing. (interview)

Similar to this last comment, another hacker builds on the point about the media's interest in making sales. He suggests that one of the main reasons why the term hacker has become synonymous with computer criminal has to do with, "...an uneducated western media that in general refuses to dig beyond the 'sex & sizzle' of any given story - that uses FUD (fear, uncertainty and doubt) to draw viewers and advertisers" (interview). From his perspective, the media attracts customers by building on the public's fear and uncertainties about hackers, even if such presentations are misleading and overly simplistic.

Fine (1987) points out that there are many cultural items widely known to a subculture that are never transmitted by the media. From his study on the pre-adolescent culture of little league baseball he argues that a great deal of common knowledge amongst this particular group (e.g., dirty jokes, sexual folklore, aggressive humour) could not be transmitted by adult-controlled mass media. He suggests that this is a result of an, "adult-controlled media, which are highly protective of children's supposed innocence and delicate sensibilities" (1987, p. 162). While this may be true of this particular culture, others have suggested that what is and is not portrayed about the hacker culture through the mass media has more to do with what is marketable rather than what is "good" for society or its

young people. Hackers themselves comment that the media is not interested in presenting an accurate picture of them, because people would not be interested in what "real" hackers look like or actually spend their time doing:

> <Steve> What's your perception on the media's portrayal of hackers?
> <Dan> The media sucks. They don't want someone intelligent, they want someone scary, sensational, someone that looks the part of a hacker. When you're smart and normal looking no one cares... (interview)

Some hackers feel that presentations of their culture differ based upon the various forms of media. For instance, the hacker in the following interview excerpt indicates that he does not have as many qualms with journalists and the print media, but feels that the video media, given their interest in coming up with eye-catching presentations, tend to focus on providing visuals of abnormal-looking individuals and present them as hackers, even if these people indicate they are not hackers:

> <Kris> ...[T]he video media singles out the physically different. I remember a friend of mine being interviewed at Defcon 2 [a hacker conference] - he has facial piercings, a mohawk, and tattoos. The whole time he kept saying, "I'm not a hacker, I don't do anything, I'm just here to see friends", but the media wouldn't hear it. He HAD to be a hacker, cuz look how WEIRD he looks. So lots of folks tried to emulate that - shave your head, pierce your lip, go to Defcon, get on teevee, get a sexy high paid job as a security 'guy'. But most of the really skilled hackers don't look like that, they can't, their jobs won't allow it. So they look normal and the video media hates that. (interview)

Media presentations are often seen as being based upon images of the "Hollywoodized" hacker (as depicted in movies like War Games and Hackers) and those individuals involved in and caught for committing computer crime and

therefore, give the culture a bad name. Some corporate advertisements, which typecast hackers as rebel adolescents, are particularly irritating to hackers:

> <Kris> Oh, don't get me started on the IBM ads. Well, too late. I was working for IBM's security team when those came out, pissed me off to no fucking end. I went to Blackhat [a hacker conference] that year and my nametag read: '13 year old sociopath'. When approached by a fellow IBMer (boss' boss) and asked what that meant, I replied, 'OH, didn't you see the commercial, that's what I am, cuz all hackers are 13 year old sociopaths. Well gotta run, I'm getting my nose tattooed'. I didn't last long at IBM... And those damn Computer Associates ads too...the 'why do we break into your networks and trash your data? For the same reasons we pierce our tongues!' commercial. God I wanted to fucking hit someone over that, possibly with a brick, or a Buick. (interview)

Hackers argue that, similar to the news media, a tactic used by computer corporations to make sales is to build upon the public's fears of the unknown world of the hacker. This is accomplished by taking advantage of people's insecurities regarding the potential threat of the those "witty kids" who know so much about the computer systems that, let us remind you, so much of people's lives have become tied to. Such advertisements serve to further stigmatize all hackers not only as security threats, but also as being malcontent youth and visibly abnormal.

Advertisements, along with movies and the news media, also create mainstream caricatures of the prototypical hacker, which become emulated by individuals wanting to be hackers. Cory is a good example of this route to involvement:

> <Steve> How did you become involved with hacking?

> <Cory> Well I saw the movie 'Hackers' and I checked a site out and it had guides to teach u how to become a hacker. And the Anarchy Cookbook has very good guides too. (interview)

In this way, outside representations of hackers provide material that may be incorporated into the culture. As individuals become interested in hacking and adopt mainstream images, they further perpetuate advertisements, and the public fear and misunderstandings, which end up stigmatizing all hackers.

Some hackers who have taken on a computer security consulting role indicate that, while they might take issue with mainstream portrayals on a personal level, "hacker hysteria" and public ignorance is good for business:

> <Steve> In general, what's your perception of the media's portrayal of hackers?
> <Bruce> Media makes me money :)...
> <Steve> What do you mean by the media makes you money?
> <Bruce> Well, when John McAfee [founder of McAfee Assoc. Inc., makers of anti-virus software] told the world that Michelangelo [virus] was going to wreak havoc on 60 million computers and erase all the data, I got a flood of clients simply wanting me to look at their organization and find an anti-virus solution that fit their way of working. That's an older example, but it's a good one. Except back then, I was still a business newbie, and had no idea how much I could charge for that info - I only charged $20/hour for it! Imaging getting a security consultant for that now! :) (interview)

## CONTESTED INSIDER DEFINITIONS OF "HACKER"

In describing the relevant actors in the computer underground[19], Arbaugh (1999) draws distinctions between the various roles played by these individuals. His presentation is necessarily simplified in that he compartmentalizes the various actors into different typologies. In outlining the roles played by these individuals, Arbaugh (1999) adopts the stance that there are in fact "true" hackers. He situates this understanding by conceptualizing the term from a historical vantage point, using the original meaning of the term (as was used by the first generation of hackers) to characterize *real* hackers and define the roles played by others in the computer underground (who may or may not refer to themselves as hackers). The problem in this, as Arbaugh (1999) hints at,[20] is that a number of members of the computer underground refer to themselves as hackers (but are not in Arbaugh's argument, as they do not fit the original definition of "hacker").[21]

[19] "Computer underground" is an expression used to describe the community of individuals who are heavily involved in the use of computers, and more particularly, computer networks. The purpose underlying this intense use of computers is often described in malicious terms, but need not be. Some researchers (*see* Taylor, 2001) use the terms computer/information underground and hackers interchangeably. Hackers do likewise. For example, the Defcon conference – a conference hosted by hackers, for hackers – is promoted as the "annual computer underground party for hackers" (Defcon, 2001).

[20] Arbaugh (1999) states that, "...crackers often like to define themselves as hackers, [however,] most true hackers consider them to be a separate and lower form of life" (p. 371).

[21] The question that Arbaugh's (1999) point ultimately raises is, who's vantage point is privileged in defining who is and is not a hacker? The interactionist take on this is to examine the act of defining and persuading during the course of individuals' direct and indirect interactions with one another. Rather than acknowledging a single definition as being privileged, it is more advantageous to explore how meaning is situationally defined.

What we find are a several competing arguments amongst members of the computer underground in defining what a hacker is. Some, like Arbaugh (1999), draw upon the original definition of the term to define hacker:

> There is a community, a shared culture, of expert programmers and networking wizards that traces its history back through decades to the first time-sharing minicomputers and the earliest ARPAnet experiments. The members of this culture originated the term 'hacker'. Hackers built the Internet. Hackers made the Unix operating system what it is today. Hackers run Usenet. Hackers make the World Wide Web work. If you are part of this culture, if you have contributed to it and other people in it know who you are and call you a hacker, you're a hacker. (Raymond, 2000a)

Others, while not specifically linking their definition of hacker to the original meaning, draw upon the ideals laid out by the first generation of hackers, such as the notion that hackers build, not break, things:

> <Matthew> An Hacker is an individual who has a driving desire to learn or improve computer systems. Generally, improvements are quick "hacks" that solve the immediate problem, but do not address the larger picture, or fit within the normal specifications of an architecture. (interview)

Still others have moved away from or built upon old-school understandings of what defines a hacker. Some self-proclaimed hackers suggest that the "old-school" definition is obsolete, as it does not reflect the new forms of activities hackers have become involved in. For the "hackers" in the next three excerpts, creating viruses, defeating network security and stealing electronic files are legitimate hacker activities:

> <Cory> Real hackers just want info.
> <Steve> Info about what?
> <Cory> Anything that could be useful, like something to sell and for your own info, like Microsoft is making a new game with id

> software (this isn't true, just an example). Or more important stuff.
> <Steve> What would you say is the more important stuff?
> <Cory> Like credit card numbers, whatever u need. (interview)

> Heh...I think that WRITING a trojan program[22] would be a step to hacker-dom. Not necessarily MAKE one a hacker, but it'd be a step in the right direction... but that's just me. (newsgroup posting)

> <George> I'm just a geek, I'm not a hacker
> <Steve> how do you distinguish between the two George?
> <George> I don't break into computer systems. (field notes)

Hackers adhering to the original definition of the term suggest that anyone who uses computer knowledge to create viruses, steal or break into a computer is a criminal, not a hacker. The following newsgroup posting shows the type of censure that arises as people ardently criticize[23] one another for misusing the term:

> hi to all the true hackers, id just like to say that i dont usually flame but most of the assholes who post to this group are a bunch of losers. With subjects like "i can hack excel and word" and all you fucking morons who think youre some kinda 31337 haxor [elite hacker] cuz youre trying to write a trojan are not hackers and you could never even begin to comprehend the meaning of a true hacker so fuck off with your viruses and your scripts and "how do i wire free money into my bank account" and "how do i hack into someones e-mail account" because you are not, never will be, and never fucking could be a hacker. you can e-mail me telling me off and you can try to fuck with me or something but i dont care because i can always fix my shit but youll always suck. (newsgroup posting)

---

[22] Named after the story of the ancient Greek Trojan horse, a Trojan (horse) program is, "A malicious, security-breaking program that is disguised as something benign" (Raymond, 2000b: 389).

[23] This type of intense online attack against another person or group of people is referred to as "flaming." The hurling of slurs and insults can quickly turn into a "flame war" as more and more people join in on the argument.

This type of flaming is often accompanied by calls for those being attacked to use the "proper" label for their behaviour (e.g., cracker, script kiddy). Take for example the following posting to a newsgroup, wherein the individuals asks "crackers" to not call themselves hackers:

> Has it ever occurred to any of you that you are in fact crackers not hackers. A hacker is generally non malicious in intent whilst a cracker enjoys cracking codes and even leaving behind or inserting potentially harmful files or viruses. Now I know this makes absolutely no difference to anybody, but at least take pride in what you do and get the damn title right. (newsgroup posting)

**Hackers and Crackers**

The differing perspectives among hackers have led to an ongoing debate as to what characterizes a *real* hacker. Such debates are played out online through IRC chats, web pages and newsgroups and offline during meetings and conferences. During these debates people attempt to draw distinctions between what a hacker is and is not. To do so, new terms such as worm, cracker, blackhat, warez d00d, cyberpunk, and script kiddy are used to label those who want to be or think they are hackers, but whose activities, mindset and skill level are not representative of *true* hackers. These terms have been promoted (with varying degrees of success) as labels for individuals who use their computer knowledge for malicious or illegal purposes.

Perhaps the most common distinction made by hackers is the difference between hackers and crackers. The word "cracker" was introduced in the early 1980s by "true" or "old-school" hackers to distinguish themselves from those

who were using their computer expertise for illegal purposes (Raymond, 2000b). In the traditional sense (i.e., as used by old-school hackers), the term hacker is used to describe a person who has exceptional technological knowledge of, and an extremely keen interest in, learning the ins and outs of computers and electronics (especially software programming). Whereas, a cracker can be defined as a person who may or may not have as much computer knowledge as a hacker, but ultimately uses his or her knowledge in an attempt to break computer security. In the following example, Eric Steven Raymond[24] distinguishes "real" hackers from crackers by maintaining that breaking computer security does not make someone a hacker:

> There is another group of people who loudly call themselves hackers, but aren't. These are people (mainly adolescent males) who get a kick out of breaking into computers and phreaking[25] the phone system. Real hackers call these people `crackers' and want nothing to do with them. Real hackers mostly think crackers are lazy, irresponsible, and not very bright, and object that being able to break security doesn't make you a hacker any more than being able to hotwire cars makes you an automotive engineer. Unfortunately, many journalists and writers have been fooled into using the word `hacker' to describe crackers; this irritates real hackers no end. (2002a)

There are two re-occurring distinctions people make when discussing the differences between hackers and crackers. The first represents an ethical or moral

[24] Eric Steven Raymond is a self-proclaimed hacker ethnographer who has worked for a number of years in the computer field. Through conference presentations, publications and information contained on his web site he has worked towards dispelling the "hacker myth" (i.e., crackers are not hackers), which he asserts has been perpetuated by the media. He indicates that the basic difference between hackers and crackers is that a "real" hacker builds things, a cracker breaks things.

[25] "Phreaking" or "phone phreaking" is a termed used to describe the different ways of receiving or making a phone service without being billed (Arbaugh, 1999). Those with an interest in phreaking are called phreaks.

stance towards the perceived intent of the individual's behaviour. The second distinction is based upon the knowledge and self-initiated problem-solving the individual is willing to invest in his or her work. Although I have already suggested a reasonably clear-cut breakdown of what distinguishes a hacker from a cracker, such an unambiguous division is problematic as it does not do adequately take into account the varying viewpoints self-defined hackers have of the two groups.

As some of the previous quotes suggest, a number of individuals argue that the goal of hackers is to do "good", or, at the least use their knowledge of computers for non-malicious purposes. With that said, some hackers suggest that this distinction is not absolute – i.e., some hackers do use their computer know-how for malicious purposes:

> <Kris> Hackers can be good or evil - intentionally or unintentionally; crackers are just evil. Crackers to me are usually just criminals with computer skills. There are 'evil' hackers though. Most of them are just crackers, but behind every army of crackers there is usually an evil hacker, kinda like the bad guy in a Bond film. Well, except the bad guys in Bond movies don't usually live in their parent's basement or drive an '82 Corolla. (interview)

For some, the difference between hackers and crackers is not an ethical or moral issue, but rather has to do with the amount of knowledge they possess about what they are doing and the disciplined way in which they approach and solve a problem:

> <Steve> Do you distinguish at all between hackers and crackers?
> <Bruce> only in the way I differentiate Good cops and Bad cops
> <Steve> So how would that be?

> <Bruce> some crackers don't know how to hack - they run a script. Some crackers definitely know what they're doing - they are hackers.
> <Steve> So the difference would be in the skill level. What about in terms of ethics? Do you distinguish between hackers and crackers at all that way?
> <Bruce> it's not an ethical question - that's why I say there are both good and bad cops. It is skill level certainly. And it is the ability to conduct their "hacking" in a manner that is methodological. (interview)

A number of hackers, adhering to the "old-school" standpoint, indicate that as soon as a person uses their knowledge for illegal purposes, they should be referred to as a cracker, not a hacker.

One thing that does hold true, and was mentioned by nearly all interviewees, is that a prerequisite for being a hacker is that one must possess an in-depth understanding of computers and strive for ever greater understandings of "what makes things work" at a base level:

> <Steve> What's your definition of a hacker?
> <Dan> A person, whether male or female who enjoys working with technology to a degree that borders on obsession. In short... someone that wants to know how stuff works. (interview)

Crackers, on the other hand, are almost always described in negative terms as being motivated by "evil" or "bad" intentions, as their goals are often selfish and have a malicious bent. While some crackers may have a significant amount of computer knowledge, you only achieve "hackerdom" if this knowledge is used appropriately. Consider the following comments:

> <Brad> A hacker is a person who explores problems and solutions, be it computers, engineering, science etc... Crackers are people that don't care about learning, or helping, they are only

> interested in what they can get for free, with the least amount of work (thief, vandals etc come to mind). (interview)
>
> <Brandon> A hacker is the one who has the knowledge to perform and invent things. If you're a hacker in optical electronics or whatever, it doesn't mean you're somebody who cracks the system or finds bugs in it, no. It means that you're very knowledgeable about this. That's a hacker. Since he's very knowledgeable by default he will find mistakes and bugs in the system. He has the chance to either report it or not... Hackers are known to report the bugs they found. So being a hacker doesn't mean now that he is a "bad guy". You know? A cracker, is a must, he is a "bad guy", even if he doesn't delete anything from the system and crash the system. But, he uses whatever the hacker developed or found in the system and posted and tries to use this to gain access for his own satisfaction or find information to sell or just to destroy the system. (interview)

Some hackers suggest that such distinctions are simply useless rhetoric. The hacker in the following dialogue suggests that individuals have become overly caught-up in seeking to justify and retain their own meaning of the word:

> <Steve> have you seen some of the discussion surrounding the differences between hackers and crackers?
> <Shawn> yeah, it's bullshit
> <Steve> how so?
> <Shawn> people justifying the use of the term hacker.. it's been romanticized (as much as you can with something that is inherently geeky) so everyone wants to retain the special groovy word.. hacker is a word.. that's it.. this cracker crap has gone overboard. (interview)

Similarly, Andy suggests that if the goal in applying a different label to malicious computer users is to "play politics" then a new label is likely to have little impact:

> <Steve> Do you make any distinctions between hackers and crackers?
> <Andy> Those are just words, like blackhat/whitehat, etc. Yes, I acknowledge that there are people that misuse information, and I don't consider them hackers, because I don't think they're in it for the pursuit of information. But to simply throw a different label

> on it and think that it's going to change things in the eyes of the media. I don't see the point in that. People will always fear what they don't understand, and that's unfortunate. Playing politics with vocabulary isn't the answer to that. (interview)

**Hats: White, Black and Grey**

As the final quote of the previous section indicates, hackers also use the terms "whitehat" and "blackhat" interchangeably with the terms hacker and cracker to distinguish between different types of hackers. The terms whitehat and blackhat were originated by members of the computer security industry to distinguish between malicious and non-malicious hackers. These categorizations have since been adopted more broadly within the computer underground. In the simplest of terms, blackhats are the "bad guys" – i.e., those who attack computer security; whereas, whitehats are the "good guys" – i.e., those protecting computer security from blackhats. The whitehat/blackhat analogy is based on old cowboy shows where white and black hats were used to distinguish the good cowboys from the bad.

Whitehat hackers include those individuals who use their knowledge of computers for non-malicious purposes such as working as professional network administrators in charge of securing companies' networks, or hackers who report computer security vulnerabilities rather than exploiting the problem for their own interests:

> <Mike> I guess I'm what you would call one of those 'white hat' people; I don't go out looking for systems to compromise, and if I do find one I always report it and let them deal with it. (interview)

A blackhat on the other hand is an individual who uses his or her knowledge of computers to find and take advantage of a computer's security loopholes or create and distribute computer viruses.

The hacker in the next interview excerpt indicates that there are actually three types of "hats." From this individual's perspective it is possible to be both a whitehat and blackhat, or as he puts it, a "greyhat":

> <Carl> I consider myself to be a greyhat. See the industry is broken down into 3 hats... Blackhat (your cracker whose purpose is break into as many networks as you can), your Whitehat (Your security engineer who does not dabble nor go anywhere near hacking tools and exploits, sticks with Cybercop and feels empowered because of his Bugtraq access. Your whitehat learned most of his security knowledge from books, papers, or University/College Extension courses:). Then you have your greyhat. There is always a grey line to everything isn't there? ;). Greyhats make up a pretty large portion of the "Hacking Scene". These guys and gals started out as blackhats and realized they had to pay rent ;). Basically protecting corporations and companies during the day, but releasing exploits and conducting vulnerability research at night. It's you're whole Dr. Jekyl and Mr. Hyde situation. (interview)

It is not uncommon for hackers to consider themselves as greyhats. Some blackhats may even stop using their knowledge of computers for malicious purposes and turn to using their skills as whitehat hackers. As some blackhats get older or begin to see the their interests changing, they turn to using their computer knowledge for legitimate financial gain:

> <Bruce> Anyway, about the online hacking...after a while, I decided it would be better to get paid than to risk going to jail, and so I got into consulting. Now my company is quite successful and I'm turning it around to open an Information Security school. By consulting, I mean security consulting - we were doing a lot of

> penetration testing, for instance, but well before I'd heard that phrase. It was just Security testing.
> <Steve> Wow, so you have been at this awhile then.
> <Bruce> I've been hacking for a long time, yea. Only now I do it legally. I love it though, because in my position, I get to hack on equipment that most people will never get to see. (interview)

> <Ryan> My perspective now is as an ex-black hat, now specializing in protecting against hackers. (interview)

In addition to whitehat, blackhat, hacker and cracker differentiations, hackers make use of additional labels to further distinguish between one another in terms of skill level and substantive computer interests. The different labels applied to individuals within the hacker culture are used not only to make indications as to the type of activity they are involved in, but also to distinguish where a person sits within the informal hacker hierarchy. Based upon one's peer recognition in the culture, he or she will be assigned a label seen to be appropriate for his or her status. For instance, the term "script kiddy", is a role label applied in the most derogatory sense to younger individuals (usually adolescents, however, the term becomes even more derogatory when applied to older individuals) who have little or no computer knowledge, use programs or "scripts" for malicious purposes and are chastised for trying to imitate the antics of popularized versions of hackers as seen on film:

> <Max> [S]cript kiddies tend to just download compile and run scripts without any understanding of what they are doing (most of once compiled you just run the code with the right -flags to gain access to a system through a weakness or a flaw in the code). gH (gLoBal He11) were a good example of some famous script kiddies. The people who download trojans and scan etc, usually don't have a clue what's actually going on they just want to be

> 'hackers' like in the films and break into someone's computer. (interview)

Although individuals may be labelled as script kiddies by others within the hacker culture, these individuals rarely ever refer to themselves as script kiddies. To do so, would mean admitting to being immature and having little knowledge about computers. In short, they would be acknowledging that they are not "true" hackers. Therefore, these individuals are more likely to refer to themselves as hackers. While people labelled as script kiddies may "deceive" outsiders into believing they are real hackers, the hacker in the following dialogue indicates that script kiddies are definitely not hackers. He invokes a medical analogy to explain the difference between a script kiddy and a hacker:

> <Steve> So, when "script kiddies" refer to themselves as hackers... what is your perspective on this?
> <Matthew> It's the same as a guy with a bottle of Tylenol claiming to be a medical doctor.
> <Steve> Interesting analogy.
> <Matthew> It works and it explains why hackers use scripts when testing security ... doctors prescribe Tylenol too ... you just have to know when to use it, and when not to. (interview)

As the following interview excerpt shows, "real" hackers and crackers despise script kiddies as they see these individuals as giving hackers a bad name:

> <Carl> Skript kiddies are a fungus :) And actually a real pain in the A$# to real Hackers and Crackers. They give bad media attention. They are the reason all of us have been stereotyped into one big clump. (interview)

The way in which an individual will be seen and treated is dependent upon the meaning a person's "hacker" label (e.g., hacker, cracker, script kiddie, greyhat) holds for an individual or group. However, the meaning attributed to a

particular label is highly relative. Given the diversity of activities and definitions that exists within the hacker subculture, this is the case for both insiders and outsiders alike. The hacker in the following dialogue explains that, although someone may hold status in their own group, their understandings of what defines a hacker may not apply in a different group. Therefore, their status within the new context could very well be diminished:

> <Steve> Are there any norms or rules of behaviour amongst hackers?
> <Kris> ya..
> <Steve> What sorts of things?
> <Kris> Depends on what 'strata' you're at in the community. For example, if newbie42@aol.com joins a channel like [mine] for the first time, he's gonna get booted if he opens up with 'wassup bitches', but if I do it, it's, 'OH, Hi, Kris'
> <Steve> So there's a hierarchy?
> <Kris> There's a very complex social structure in the hacker world... It's very hard to define because each 'strata' has their own set of protocol for dealing with each other and folks from other stratas... Like at the top of the food chain, the realm of the truly elite hacker, they interact with each other as normal people, there's no bullshit, nothing. But at the bottom of the pyramid, the skript kiddies have a very complex social structure that's a hierarchy of perceived power/influence
> <Steve> So each strata can have a hierarchy within itself and also can be grouped and seen somewhat hierarchically in terms of the different groups... elites down to kiddies.
> <Kris> Yup, and it's funny to see how other stratas interact with each other. For example, if I cruise down to the skript kid level, some places will abuse the crap out of me because in their power structure, I'm no one, but in other levels, I get their weird frightened/respect, because I'm one of the [conference] organizers. (interview)

Each small group of hackers may form around a more specialized type of "hacking" such as software programming, website defacement, pirating software or "hacking" the phone system (i.e., phreaking). While these individuals may be

assigned greater or lesser status within the "overarching" hacker subculture, each local subculture develops its own set of definitions, perspectives, and norms.

## DISCUSSION

This chapter has highlighted the importance of going to hackers to better understand how they define themselves and how they interpret outsider representations of their subculture. As Huss (1998) has also found, hackers blame the media in particular for their public image problems. Hackers see media portrayals as often presenting a one-sided view of the hacker community. They criticize the media for inaccurately attributing the activities of computer criminals to hackers. Rather than presenting a picture of the more "mundane" and thus, less newsworthy world of "real" hackers, hackers state that the media, given their sales agenda, focus on the visibly abnormal and computer criminals who call themselves hackers. Hackers also argue that computer companies, through their advertisements, build upon this general stereotype and people's fear of the seemingly mysterious realm of the hacker in order to increase sales of their security products. Similarly, Huss (1998) indicates that hackers believe that the media presents extreme cases of "hacker" activities in order to create drama, "...to stimulate the interest of a public with limited understanding of computers and hackers" (p.50).

In characterizing hackers as being a certain type of individual -- typically adolescent, rebellious, dangerous, and visibly abnormal -- popular discourse and images tend to stigmatize all hackers as being deviant. Likewise, Huss (1998)

points out that, "[Hackers] generally agree that both printed and television news accounts confuse computer crime with hacking and contribute to a negative image of all hackers" (p. 53). At the same time, these images present caricatures of the prototypical hacker that those aspiring to be "hackers" often end up replicating. This point relates directly to Fine and Kleinman's (1979) assertion that, "Through the media, adolescents, learn the behaviors and norms of peers, who, through their prominence in the media, become role models" (p. 15). In this way, those promoting mainstream representations provide material that may become incorporated into the hacker culture more broadly. This occurs particularly through the new involvements of individuals who define themselves in terms of mainstream definitions. By condemning the behaviour of those engaged in "countercultural" activities, Fine and Kleinman (1979) argue that media messages may actually activate its spread, a process referred to as deviance amplification. While some hackers indicate that they may take issue with such stereotypical portrayals on a personal level, those hackers acting as security consultants suggest that "hacker hysteria" and public ignorance surrounding computer security are good for business.

This chapter has also drawn attention to the ongoing debate within the hacker community about what defines a hacker. Some suggest that the original "desire to learn and improve computers" definition still applies, while others indicate that such a definition is somewhat outdated and does not consider the extension of the hacker mindset to new forms of activities such as virus creation

and software piracy. As Huss (1998) notes, some hackers agree that certain types of activities they engage in are, by *outsider* definitions, criminal. However, those advocating the traditional definition maintain that, while there may be some grey areas, there are ethical and legal limits dictating how far one should go in applying their creative, problem-solving approach. These individuals suggest that activities with a malicious or illicit bent are no longer *hacker* activities, but the behaviour of *crackers* and *criminals*.

In order to help situate others within the community and define who is and is not a hacker, a series of terms have been adopted and applied to those considering themselves to be hackers. This chapter argued that one significant labelling distinction hackers make is the separation of individuals into two broad categories: hackers and crackers. The main distinguishing characteristics used to define these two groups are the imputed (a) ethics underlying the intent of their behaviour and, (b) level of knowledge and self-initiated problem-solving which they demonstrate. This finding coincides quite closely with Huss' (1998) research, which suggests that hackers distinguish between one another according to their "level of skill" and "degree of maliciousness" (p. 87). Based upon these criteria, hackers are characterized as those who apply their higher degree of computer knowledge and problem-solving ability for non-malicious or "good" purposes (e.g., software development, network security); whereas, crackers are characterized as typically, but not always, being less computer savvy and engaging in malicious activities (e.g., virus creation and distribution, unauthorized

network infiltration). Terms such as *whitehat* ("good guy") and *blackhat* ("bad guy") serve similar purposes in distinguishing between the perceived morality behind people's computer activities. The term "greyhat" is a title given to hackers who dabble in both whitehat and blackhat activities.

By drawing definitional boundaries between others in the community, hackers engage in a constant negotiation of their social reality with not only outsiders, but also other insiders. Dependent upon what group one is part of or enters into, their label and its accompanying meaning may hold more or less weight. The various label designations or "role labels" (examined further in the chapter on hacker argot) are used by hackers as ways of understanding and explaining to others where people are situated within the culture. These labels act as quick identifiers, each with their own set of shared meanings. By differentiating between individuals in terms of such things as their imputed level of knowledge, the activities they engage in, their motives and, more generally, how they apply the term hacker, hackers form their own group or *local subculture* perspectives and identities. Understandings of what constitutes a hacker, therefore, are dependent upon the reference group an individual chooses to anchor his or her definition of hacker to.

Furthermore, in distinguishing the different subcategories of hackers in terms of characteristics such as their criminal (cracker) and non-criminal (true hacker) activities, hackers attempt to neutralize the stigma associated with their deviant public identity. By drawing clear distinctions between what a hacker is

and is not, hackers challenge outsiders' perceptions and actively work to distance themselves from their alleged deviant status. A slogan advocated by Eric Raymond is poignant in this regard. In order to help dispel the hacker myth and work towards returning "hacker" to its original meaning, he asserts, "Don't worry I'm a hacker, not a cracker." When further associated with another of his mottos, "Hackers build things, crackers break them", one is able to situate the meaning underlying the hacker and cracker labels and possibly develop a conception of hackers as non-malicious and crackers as malicious. Even with such efforts, as hackers themselves admit, given their diminished status in the claims-making game and the predominant anti-hacker sentiment that exists within the public domain, which is in turn reinforced by the media, the computer security industry, governments, and even certain groups of hackers, traditional hackers have by and large lost control of outsider impressions of their subculture.[26] Given the entrenchment of such widely held outsider beliefs, *all* hackers will likely remain the scapegoats of computer crime for some time to come.

The next chapter further explores the ways in which meanings are applied within the hacker subculture by analysing the hacker ideology. As with the definitional issues examined in this chapter, the next chapter provides an analysis of the principles underlying the hacker ideology and how these principles are appropriated to suit the different local subcultures of the hacker community.

---

[26] As mentioned, Huss (1998) makes a similar assertion: "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" (p. 74).

# CHAPTER FIVE

# THE HACKER IDEOLOGY

*Denoting interpretive frameworks or viewpoints (also worldviews, paradigms, versions of reality) for making sense of the world, the perspectives that people develop through association with others provide the orientational content of group life. (Prus, 1997, p. 62)*

## CONCEPTUALIZING IDEOLOGY

A major characteristic distinguishing a particular subculture from the broader community is its ideology or group perspective (Fine & Kleinman, 1979; Prus, 1997; Shibutani, 1955). An ideology represents a unique way of understanding the world, which tends to justify what the subculture is all about. Within the hacker subculture, this ideology is sometimes referred to as the "hacker ethic" or "hacker spirit."

As Shibutani (1955) indicates, shared perspectives arise through participation in common communication channels, which form the boundaries of a group's subculture. Therefore, in order to comprehend an individual's perspective, it is necessary to understand the social world(s) in which he or she is a part of (Shibutani, 1955). It is within the shared group context that individuals form relationships with others who share a similar perspective, which in turn support, reinforce and sustain particular viewpoints.

Individuals might simultaneously be involved with a number of different sub-societies adhering to a variety of different perspectives. Through these interactions, individuals develop a number of similar and dissimilar viewpoints, and engage in an ongoing negotiation and (re-)formulation of reality:

> ...[I]ndeed, each member's perspective on the shared knowledge of the subculture will necessarily be different from that of any other member. Therefore, even within a homogeneous group, action will require a negotiation of meaning, resulting in the continual production of socially constructed realities – a continual shading of the "culture of the group." (Fine & Kleinman, 1979, p. 6)

> [S]ocial worlds are not static entities; shared perspectives are continually being reconstituted. (Shibutani, 1955, p. 567)

Social worlds and the accompanying perspectives individuals derive through interactions within group contexts can therefore be envisioned processually and in a more or less constant state of flux. Intersubjective understandings toward the world are not only relative across time and between groups, but since individuals develop their own personal understandings of the world through self-interaction and interpretation, perspectives may also differ from individual-to-individual. While noting some distinctions, this chapter is concerned with the hacker ideology as it is shared more generally between insiders and subsequently described to outsiders.

Shibutani (1955) maintains, "A reference group... is that group whose outlook is used by the actor as the frame of reference in the organization of his perceptual field" (p. 565). Following this line of reasoning, by examining hackers as an imputed reference group, it is possible to distinguish the hacker perspective

from other perspectives. That is, it is possible to observe the hacker perspective as it is described and invoked by individuals in their conversations with others (hackers and non-hackers included), as they take stands on certain issues, convey understandings, and describe their viewpoints to others. By observing and interacting with hackers one comes to understand how they use their perspective to justify certain ideas and rationalize the appropriateness of different courses of action.

While a perspective may be reflected in an individual's actions, this does not necessarily need to be the case. A perspective may remain at the level of ideas (i.e., not be acted upon), shared with others through language or be observable in the ways individuals interact with others and the world more generally. In this way, ideologies may not move beyond mere rhetoric – ideals that one professes to strive for, but never acts upon. This chapter reflects the hacker ideology as it is *described* by self-proclaimed hackers.

## THE HACKER SPIRIT

In Steven Levy's (1984) book, "Hackers: Heroes of the Computer Revolution" he identifies the following components of what he has termed "The Hacker Ethic":

- Access to computers – and anything which might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-On Imperative!
- All information should be free
- Mistrust Authority – Promote Decentralisation
- Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.

- You can create art and beauty on a computer
- Computers can change your life for the better (pp. 40-45).

Taken together, elements of the Hacker Ethic, as described and argued by Levy (1984), represent the ideology of the first generation of hackers. Data from this thesis suggest that these principles have remained more or less consistent across time. Support for this claim is bolstered by the recent findings of Arbaugh (1999). In discussing the shared beliefs and norms of the hacker subculture, Arbaugh (1999) indicates that, although there might be differences between different "types" of hackers (e.g., script kiddies, crackers, "true" hackers), the beliefs that, "one should acquire as much knowledge as possible, that all information should be shared, and that all information should be free" (p. 377) hold true among all hackers.

In my discussions with hackers, the phrase "hacker spirit" was often used as a label for their particular perspective or ideology. In order to remain true to the language used by participants, I will use "hacker spirit" to refer to the combined features of the hacker ideology imputed by those involved in this research. Very similar to Levy's (1984) "Hacker Ethic", seven fundamental and interrelated elements of the hacker spirit were observed in analysing the data for this thesis. Each element is based upon an overarching goal: *striving for an ever-greater understanding of how things work.* To hackers, knowledge and an unorthodox approach to learning are valued above all else. Consistent with this goal, the following principles represent the essence of the hacker perspective:

1. Higher understanding requires an unorthodox approach – be inventive, think outside the box;
2. Understanding things, solving problems and generating new ideas requires hard work – dedicate yourself to this task;
3. Learning should be self-directed – learn by doing;
4. A hacker's learning time is precious – share your knowledge with others;
5. You are evaluated on what you know and how you learn – looks and degrees are not important – show us your skill;
6. People in positions of power often value and impose conformity – this attitude must be rejected as it stifles creativity – mistrust authority; and,
7. Hackers require as much information as possible to understand things – access to information should be free and unrestricted.

What follows is an examination of each of these ideological principles as related by hackers.

**The Hacker Spirit: The Pursuit of Knowledge**

> *A [computer] user is involved with the machine in a hands-on way, but is not interested in the technology except as it enables an application. Hackers are the antithesis of users. They are passionately involved in mastery of the machine itself. (Turkle, 1997, p. 32)*

Rather than the hacker ideology being something that a person applies only at certain times in specific situations, hackers describe the application of their perspective as "a way of life." The pursuit of knowledge and how one goes about learning are the key aspects of this particular way of life. Hackers are not content with the taken for granted ways of using things. Instead, they believe in seeking to understand things for themselves and using objects in new inventive ways. The hacker in the following dialogue indicates that the key trait of being a hacker is trying to understand everything a person can get his or her hands on:

> <Steve> How long would you say you've been a hacker?
> <Brad> all my life

> <Steve> You were born a hacker?
> <Brad> I'd have to say I was. I remember being 3 or 4, and taking apart my remote control cars to make them go faster. Though, I don't think one has to be born a hacker, they just have to have a desire to understand everything they get their hands on. (interview)

In pursuing an understanding for how things work, hackers believe that one must start with the perspective that anything is possible and that people should not be restricted by others' ideas. To achieve this sort of understanding, the hacker in the next excerpt describes that hackers picture things in terms of "raw components" and then work towards conceptualizing and building things from the bottom-up, rather than the top-down:

> <Kris> A hacker is someone who puts things together without reading the instruction manual. Hackers view things in terms of raw components. You might get the set of Legos to build a pirate ship, but discover you can also build a seaplane out of the parts. As a result, hackers can do very good things or very bad things. When it comes to computers, it's the same mindset: I can do anything with this machine, even if you (i.e. Microsoft) haven't given me the ability to, I'll find a way. It's the urge to take things apart and see how they work. (interview)

Another hacker explains, to be a hacker is to not be content with others', or even your own, knowledge of how things work:

> <Mike> I was never satisfied with knowing 'only what I knew at the time'. It's like a hunger for knowledge; taking something apart to see how it works - only in software. (interview)

Consistent with this perspective, he maintains that:

> <Mike> [A hacker] is someone who's technically oriented with a high learning curve who isn't satisfied with the 'off the rack' version of what things are, how they work, and how they should be used; someone with a genuine wanting to know how things work on a low level... (interview)

What follows is a description of each of the ideological principles underlying the hacker spirit.

***Principle #1: Higher Understanding Requires an Unorthodox Approach***

Terms such as "creative", "unorthodox", "obsessive", "intense", "passionate", "exploratory", "curious", "relentless", and "self-directed" are common adjectives used by hackers to describe their approach to understanding. The essence of the hacker spirit involves a passion for applying one's technical ingenuity to work towards an ever-greater understanding of how things work. Part of striving for this higher understanding is to develop creative new pieces of technology such as computer programs and electronic devices, engage in the solving technical problems, and pursue different ways of using objects. This may involve coming up with "...sudden ideas on how to use something for which it was never intended", describes a hacker.

From the hacker point of view, striving for ever-higher levels of understanding and solving very technical problems requires a different way of thinking about and approaching a problem. Hackers often describe their approach as "unorthodox" or "creative." It is also not uncommon for hackers to define the term *hacker* as, "Someone who thinks outside of the box" (interview). For the sake of intellectual challenge a hacker may devote him or herself to a project that others were unable to solve or complete. The hacker in the next interview excerpt describes that overcoming obstacles when problem-solving requires that people

re-think their approach and think a bit more unconventionally about how the problem can be solved:

> <Andy> It always comes back to thinking just slightly outside of the box, something a little unconventional, something so easy, yet so absurd you wouldn't have thought of it if you kept going down the track you had been on. (interview)

She offers the following example of one of her current projects where she believes that applying a different way of thinking about the project will lead her to completing the task where others have failed:

> <Andy> My current project is something that was tried before in a commercial setting, and failed. I'm making it free, and I think I can pull it off, because I'm utilizing a structure that the original designer didn't consider; something so obvious, yet not something you would have thought of for a project of this nature. (interview)

In order to think like a hacker, one of my informants suggests that one has to learn that:

> <Brad> Square pegs fit in round holes. You have to learn to think sideways, upside down and inside out, and that there's more than one right/wrong to do the same thing, not everything is as it appears. The technical side just sort of comes with time and trying and reading and doing. (interview)

As he points out, along with taking an imaginative approach to problem-solving one also has to realize that solving problems requires time and hard work, a topic to which I now turn.

*Principle #2: Hacking Involves Hard Work*

To hold true to the hacker spirit, it is necessary to thoroughly dedicate oneself to whatever project he or she may be working on and work passionately

towards understanding. Raymond describes the intensity of this desire by comparing the work ethic of hackers to successful, highly motivated athletes:

> Being a hacker is lots of fun, but it's a kind of fun that takes lots of effort. The effort takes motivation. Successful athletes get their motivation from a kind of physical delight in making their bodies perform, in pushing themselves past their own physical limits. Similarly, to be a hacker you have to get a basic thrill from solving problems, sharpening your skills, and exercising your intelligence. (2000a)

During a meeting with a group of hackers I became involved in a conversation about the hacker perspective with one of the attendees. He described to me the obsessiveness with which a hacker will approach and dedicate him or herself to a project. He maintained that hackers routinely become so engrossed in their current project that everything else will seem inconsequential, including hygiene and sleep:

> Marvin told me that one of the hacker characteristics is devotion to a project. He said it's not uncommon to find a hacker wallowing in his own filth after staying up for 48 hours straight on a project. (field notes)

So intense is the hacker drive to understand and realize the completion of a project, that it is not uncharacteristic for a hacker to, "...work on something for weeks without sleep/food/drink," describes another hacker (interview). Although somewhat of an exaggeration, it does point to the perspective that, understanding things only as a hacker can, requires an intense dedication and focus on learning and solving problems that borders on obsession. Even though a project might pose certain obstacles and can be extremely frustrating at times, hackers maintain that it is exactly this sort of challenge that inspires them. One informant

indicates, "A hacker is a person who loves a challenge, and loves knowledge and the ability to gain it" (interview).

As a graduate student at MIT in the 1970s, Turkle (1997), a sociology of technology professor at MIT, recalls observing the intensity with which the hackers there devoted themselves to their computer work:

> In 1977, I often worked late writing at a networked computer terminal at MIT's 545 Technology Square, also known as Tech Square. My text would be printed on a laser printer on the ninth floor, which was also the site of the workstations of the legendary Tech Square computer hackers. On my way back and forth from the laser printer, I would pause to observe their intensity of concentration. They seemed not to move from hour to hour through the night, their screens usually filled with line after line of computer code. (p. 154)

To be a hacker one must incorporate this work ethic into their perspective. With that said, some hackers argue that many so-called hackers – i.e., mainly the younger generation of media-dubbed hackers – do not aspire to the hacker work ethic. They are often criticized for being lazy and ignorant. These individuals are typically labelled as script kiddies for their lack of knowledge about computers and often young age and immature behaviour.

### *Principle #3: Hacking Requires a "Learn for Yourself" Approach - Learn by Doing*

To be a hacker, the individual has to be willing to learn for the sake of learning. Much of this learning is not something that others can teach but rather something that must "come from within." As such, many hackers suggest that one needs to either begin with or adopt a "learn for yourself" mindset:

> <Steve> What sorts of things did you have to learn to become a hacker?
> <Matthew> Simple answer: I had to learn how to learn…There is no amount of knowledge that can qualify you as a hacker, or a newbie, or what have you. It all comes down to a willingness to learn new things, and a drive to learn them without being told, "Just do this because it works". Anyone can run a script or a security package like NESSUS - all you do is press "go" and it works. It all comes back to whether you are willing to learn what the program is doing behind the scenes so you can accomplish something with it. (interview)

The belief is that it is impossible to teach someone how to hack. As one hacker puts it, "You hack to LEARN, you do not LEARN to hack" (web site). Another hacker reiterates the point that hacking cannot be taught, but rather must be a part of a person's mindset – i.e., the individual has to be motivated to understand things and think creatively: "…don't come to me and say 'teach me how to hack'. Don't even say 'show me where to start', because I can't share that. There's no way that I can explain what goes on inside my head" (interview). The term "hack" used in this way can be defined as, *passionately and creatively working towards a solution to any given problem.*

As another hacker notes, one adhering to the hacker spirit is a person who must see and do things for him or herself, rather than being told how to do it: "I'm a show me rather than tell me kind of person" (interview). Following this line of thinking, hackers take the stance that self-directed understanding requires a hands-on approach:

> <Bruce> In addition, hacking is also learning a technology using hands-on methods - like the guys you're talking to that have been spending days compiling a kernel, and trying to figure out why it didn't work as they expected. (interview)

In becoming part of the hacker community, one quickly learns that many groups of hackers disdain people who do not first try to understand something on their own. Instead of engaging a problem by themselves and seeking their own solutions, a number of individuals approach hackers asking for a quick answer. This type of person is often heavily criticized:

> ... I can't speak for the other newsgroups... but people come here expecting to be spoon-fed. I have yet to see somebody flamed in here if they have done their research and simply can't find an answer to their problem. But we get so many halfwits in here asking things like "I need a crack for WinZip" and stuff like that, that flaming them becomes more or less a natural reflex... Again, I can't speak for the other groups, but we certainly don't cater to the whims of idiots, morons, halfwits and retards here. (newsgroup posting)

If people are able to show that they have done their homework, a hacker will likely be more receptive to helping them find an answer:

> <Kris> It gets frustrating when a kid asks for help with something and you find the answer by going to Google [a web site search engine] and searching. Then you tell them to try Google first next time and you get a 'fuck you'. I like the kids that try to figure out this stuff first on their own and then, and only then, do they go ask for help when there's no other choice. (interview)

***Principle #4: Share Your Knowledge and Information with Others***

Another central tenet of the hacker spirit is the belief in sharing knowledge and information to help solve problems. Raymond (2000a) argues that it is the hacker's duty to share information and solutions to problems so that other hackers can focus on solving new problems:

> To behave like a hacker, you have to believe that the thinking time of other hackers is precious -- so much so that it's almost a moral duty for you to share information, solve problems and then give the solutions away just so other hackers can solve new problems instead of having to perpetually re-address old ones. (Raymond, 2000a)

As a community that covets knowledge and the ability to gain it, the sharing of information is particularly important. Raymond (2000a) argues that the hacker community is a "gift culture." He explains that,

> You gain status and reputation in it not by dominating other people, nor by being beautiful, nor by having things other people want, but rather by giving things away. Specifically, by giving away your time, your creativity, and the result of your skill. (2000a).

Similarly, another hacker describes the hacker community in the following way: "Everyone shares with everyone. It's a community of knowledge" (interview).

The hacker community is indeed a knowledge-based society. However, "sharing" and "knowledge", as well as the appropriate use of information, hold different meanings to different members of the community. As was previously noted, there are particular pathways to acquiring information, which one must follow in order to be privy to certain forms of knowledge. Additionally, one must also abide by the informal rules of hacker etiquette for a given group, which often are only made known by interacting with or directly observing its members. Sometimes these rules are disseminated by the group via a web page or newsgroup. Even if these rules are made known in this way, the operational norms of a particular group can only truly be learned as one experiences the social dynamics of group interaction on a firsthand basis.

Depending on the group of hackers one is interacting with, various types of information are valued differently. For hackers adhering to old-school hacker ideals, information that helps one code and or find solutions to particular technical problems are of greatest import. This information is valued as it essential in the development and trouble-shooting of software programs. At the other end of the spectrum, warez d00dz place value on information that allows them to defeat security on proprietary software (e.g., serial codes, registration keys, software "cracking" programs). Such information permits them to gain access to a greater number of copywritten software titles and trade these programs with others for new information or other cracked programs. Crackers see information regarding program exploits as particularly important as it permits them to take advantage of others' computer security and possibly acquire access to confidential information.

To certain hackers information acts not only as a form of knowledge-based currency, but also becomes a form of social currency upon which reputations are based. The hacker in the next interview excerpt explains that some hackers will share information to acquire knowledge, whereas others will do it to show-off or make money:

> <Steve> Is it a big thing to get your stuff out there [e.g., information about a computer security flaw you found]?
> <Brandon> People act differently about this. Some people get really overjoyed and start talking about finding something. Especially if you're starting to be a hacker, like when you've found your first bug. Most of them want to show people that they've started to find bugs. After awhile you will start to find out that this is valuable information for you. You might benefit from it more than just by showing-off, depends on what your intentions are... So you say, "Yeah, I'll give this out to other

> people." Or, "No, I won't do it. No I want to get information and sell it..." So, it depends... Some people will do it for knowledge and some people will do it for showing-off. (interview)

When approaching different types of hackers for information, one has to know what information they value and engage them in a manner that is conducive to having them share their information. The following summary of rules from a hacker newsgroup's Frequently Asked Questions (FAQ) page is a good example of the conduct norms propagated by a particular group of hackers. The rules pertain not only to acquiring information, but also how to engage in the group's online culture:

1. Read the newsgroup for two months before posting.
2. Make posts factual and meaningful.
3. Keep your posts on topic for this newsgroup.
4. Send personal replies via e-mail, do not post them to [this newsgroup].
5. Quote responsibly. Not too much, not too little.
6. State what homework you have done before resorting to asking on [this newsgroup].
7. Do not use [this newsgroup] for software piracy.
8. Check the [the newsgroup's] FAQ before posting a question. (web site)

While the FAQ details help to better situate someone approaching the group about sharing information, as the author of the FAQs indicates, you might still be arbitrarily criticized:

> If you keep these rules in mind and abide by them faithfully, you will still get flamed [i.e., criticized]. However, you will be able to retaliate with a clear conscience that you have done everything possible to protect the social culture of [the newsgroup]. (web site)

***Principle #5: You're Evaluated Based on what you Know and your Desire to Learn***

Within the hacker community, the belief is that people should be valued based upon what they know and their creative, self-directed approach to learning and understanding. One hacker describes, "The thing that I use to judge people is their Quest for Learning" – are they genuinely wanting to know or are they just doing it for attention? (interview). Hackers place a very high value on wanting to know for the sake of understanding. Instead of valuing people based upon their looks, sense of style, or even school-earned credentials, hackers ascribe to the perspective that you will be evaluated based upon what you know and your hacking ability. Clothes, looks and degrees are seen as superficial. Hackers are impressed by people's intellect and display of skill as these things serve as markers of your pursuit for higher understanding. Take for example the following quotes:

> <Andy> In grade school, I was teased for my lack of style and grace, but this is a new era, and in my world, you'll be taunted endlessly for your lack of intelligence. (interview)
>
> ...when you play the hacker game, you learn to keep score primarily by what other hackers think of your skill (this is why you aren't really a hacker until other hackers consistently call you one). (Raymond, 2000a)
>
> <Dan> It's a sub-culture where your brain gets you accepted, not your name, clothes, or car you drive. You are cast out for being stupid, not for having Keds on instead of Nike. It's like I always say, "I have no patience for ignorance", and I don't. (interview)
>
> <Steve> What got you interested in computers?

> <Ryan> I've moved around a lot throughout my life. Computers were always there. Friends I made online never left when I moved. Computers also never judged me. They were always there for me. People online also didn't judge me by my age, what I look like, or what I wear. Instead, I was judged by my intellect. (interview)

> <Brad> My perspective is: knowledge is power, and if you don't have it, you're lost. (interview)

Accordingly, as these people mention, ignorance tends not to be tolerated by hackers. However, it is necessary to qualify these statements. Hackers who have been around the scene for a while note that when they first became involved in the hacker community, a display of wit and skill was essential to becoming accepted. As the next interviewee indicates, he had to follow a certain protocol and prove himself as a worthy recipient of the hacker title:

> <Kris> Socially: I had to show that I was worth teaching. I tried to answer my own questions and would only ask questions if I knew they would be stumpers. Experienced hackers like being stumped by the newbies. Once I was able to demonstrate that I tried to solve my own problems, I had some skills, and was a personable guy, I was accepted into the fold. (interview)

However, he, along with other hackers, notes that the emphasis on being able to demonstrate one's intellect does not seem to be as important to the current generation of hackers. He points out that all that really seems important to these younger individuals is their ability to look like a hacker and do the superficial things necessary to make people think they are hackers:

> <Kris> These days they think all you have to do is get a 2600 [a hacker magazine] t-shirt and go to a Defcon and now you're accepted as a hacker, but in some (sad) ways, they're right... We used to be this isolated community of self-important elitist bastards. We respected intelligence and derided stupidity. Now

> we're awash in mediocrity. These days they gain social acceptance by following the 'hacker' herd: hate the folks that the 'scene' hates, use the OS [Operating System] the 'scene' uses, like the culture the 'scene' likes and you'll just sort of blend in. (interview)

***Principle #6: Mistrust Authority***

Raymond (2000a) points out that an essential component of the hacker spirit is a tendency to be suspicious of those people who hold power in our society. He indicates that the reason for this attitude is because authority tends to abuse its power and ultimately stifle creative development:

> Hackers are naturally anti-authoritarian. Anyone who can give you orders can stop you from solving whatever problem you're being fascinated by -- and, given the way authoritarian minds work, will generally find some appallingly stupid reason to do so. So the authoritarian attitude has to be fought wherever you find it, lest it smother you and other hackers...Authoritarians thrive on censorship and secrecy. And they distrust voluntary cooperation and information-sharing -- they only like `cooperation' that they control. So to behave like a hacker, you have to develop an instinctive hostility to censorship, secrecy, and the use of force or deception to compel responsible adults. And you have to be willing to act on that belief. (Raymond, 2000a)

Hackers value the ability to think independently and not have others tell them, "This is how it should be done." People with authoritative attitudes are seen as holding hackers back from what they are good at, namely solving problems and creating new pieces of technology. The pressure to conform, which hackers suggest is rampant in all public institutions (e.g., the school system, government), impinges on independent thought:

> <Steve> How long would you say you've been a hacker?

> <Andy> How long... I suppose since I could form independent thought. I've always been the rebellious type, I refused to let the school system keep me from exploring... (interview)

As was noted previously, in order to learn about how things work, hackers take the stance that it is necessary to challenge taken-for-granted understandings. People in authority are often seen as standing in their way and interfering with learning and therefore, must also be challenged:

> <Kris> I think the hacker mindset is to challenge everything. Always push the button that says 'do not push', always try the door to see if its locked, always challenge authority, especially when it claims to be acting in your best interests.
> <Steve> Do you see yourself holding to this particular mindset?
> <Kris> Yup, even when it gets me in trouble. It's almost an obsessive-compulsive thing at times. When it's a part of you, it's involuntary. (interview)

As the hacker in this last quote suggests, being a hacker means internalizing the hacker ideology. It becomes second nature to challenge authority figures, as their rules tend to infringe upon the hacker's perspective and way of life. Because hackers challenge authority and rebel against conformity they are often seen as being deviant. While the hacker perspective is seen as abnormal and often looked down on by outsiders, hackers see their ideology in a positive light:

> <Kris> I don't see it as deviant, society does. Challenging social conventions, questioning authority, refusing to accept the 'norm' are all very positive traits to me, but society is afraid of those people. Historically, society has never liked people that 'rocked the boat' till long after they were gone. (interview)

One gets a sense from speaking with hackers that they believe those outside the hacker community actually value the hacker perspective, but are unwilling to actively work against an overwhelming societal push to conform. Quoting the

lead singer of the rock band, the Sex Pistols, one hacker states, "you will condemn in me the things you love the most" (interview).

When asking hackers about their perspective, a number of them cited a widely disseminated document on the Internet going by titles such as, "The Conscience of a Hacker", "The Hacker Manifesto" and "The Mentor's Last Words" (see Appendix B). In the document, the author, using the pseudonym, "the Mentor", criticizes society for not being able to relate to the hacker mindset. He argues that, instead of authority figures (e.g., teachers, law enforcement, governments) acknowledging and fostering hackers' superior intellect, curiosity, thirst for knowledge, and problem-solving abilities, hackers are written-off as criminals and attempts are made to force them to conform.

Although some hackers see "The Hacker's Manifesto" as being somewhat cliché or overzealous, a significant number suggest that the Mentor's words epitomize the hacker spirit:

> <Terry> You might want to look for a document out there known as "The Mentor's Last Words", or alternatively "A Hacker's Manifesto". Each version you find has a few words different due to editing ambiguities but the idea is the same. It's one of the most famous (and jokingly controversial) documents out there. Many of the more jaded of us treat it as fundamentalist babbling but its flaws, if anywhere, are in its overzealousness rather than its accuracy. It does a fair job of describing, possibly literalizing, the "hacker spirit." (e-mail correspondence)

Although not every hacker interviewed for this thesis agreed with all aspects of the "The Manifesto", they often suggested that a reasonable portion of what the Mentor was saying is consistent with their own perspective and experiences:

> <Ryan> [The Hacker's Manifesto] is quite a good description of the hacker ideology, it spoke directly to me anyways. It relates largely to what my life has been like, and my perspectives... (interview)

The Mentor's discussion regarding the misunderstood intellect of the hacker is an aspect of his writing that a number of hackers say they can relate to. The Mentor (1986) writes:

> ...Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...
> Damn underachiever. They're all alike.
>
> I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."
> Damn kid. Probably copied it. They're all alike...

Connecting almost directly with these words, one hacker indicates that this section of the Mentor's text was something that helped him feel like he was not alone, that while he may be different from other kids for being smart, there were people like him that could relate to his experiences:

> <Steve> Can you relate to what he [i.e., the Mentor] said?
> <Dan> Exactly. I have a 158 IQ, but barely passed in school. Bored. Funny too because I failed math in 6th grade because I did the math in my head. Teacher wasn't pleased, said I was cheating, wanted me to show the work, said I needed a tutor. Imagine that.
> <Steve> Are you the Mentor!?
> <Steve> hehe
> <Dan> haha
> <Dan> No, but I related to it. It made me feel better about myself, that I wasn't alone and that I wasn't a freak for being smart. (interview)

In discussing "The Manifesto", another hacker explains that she can relate to a number of the ideas espoused in the document. In particular, she argues that the

public school system saps children of their "natural" curiosity and forces them to become automatons to authoritative rules:

> <Andy> Because we value the pursuit of knowledge, we understand the burden that society places on us to conform, which leads to a rather anarchist perspective, and other conclusions follow, such as the right to privacy, freedom of information, etc... [In the public school system] children are not taught higher level thinking skills. They are not taught how to think for themselves, but rather how to regurgitate what they are told. They are being trained as drones. Children are naturally curious, until the school system beats that out of them... It's refreshing to see a child who thinks for herself, rather than simply one who regurgitates facts... They don't want resourceful, they want you to follow directions. (interview)

Some hackers disagree with the "The Manifesto." One hacker indicates that he feels that most of what the Mentor is saying is untrue, that it is outdated and it gets used in the wrong way to justify inappropriate behaviour:

> <Shawn> The problem [with the Mentor's Last Words] is it helps younger kids justify crap they shouldn't be doing...Most start off with the Mentor's Last words in mind, but a lot stop believing in it, because it really isn't true
> <Steve> What about it isn't true?
> <Shawn> Most of it...It's outdated and gets impressionable people thinking the wrong way. (interview)

As he describes, for those hackers who are involved in illegal activity (e.g., crackers, warez d00dz, script kiddies), the anti-authoritarian attitude becomes used to justify their criminal behaviour.

The perspective that "those in authority should not be trusted" becomes a heuristic device for understanding and interpreting people and their behaviour. Take for example the "mistrust authority" perspective as it was applied during one of my meetings with a group of hackers. A telephone technician was supposed to

show-up at the meeting, but he never did. This was somewhat of a letdown, but also a relief for members of the group as they suspected that he might only be attending in order to "sabotage" the meeting. One person commented:

> If the guy did show up, he might only stay long enough to point us out to the police. (field notes)

This general mistrust or suspicion of authority impacted somewhat on the data collection for this thesis, at least initially.

During my online chats with hackers, I found that they were somewhat suspicious of my intent and true identity. They were apparently worried that I may be an undercover police officer or someone who would turn them in to the authorities. The following is an excerpt from an interview I conducted with a hacker from the United Kingdom:

> <Steve> Do you have any questions before we start?
> <Max> Nope.
> <Steve> All right.
> <Max> oh wait.
> <Steve> yup?
> <Max> ARE YOU A LAW ENFORCEMENT OFFICER OR IN ANYWAY AFFILIATED WITH LAW ENFORCEMENT? I have to ask that! (interview)

Sometimes this anti-authoritarian perspective remains at the level of mere suspicion. However, it is also quite common for hackers to openly express their resentment towards computer corporations (especially Microsoft), government, and law enforcement. The reason behind this resentment, as one hacker explains, is that companies such as Microsoft are seen as representing and imposing conformity:

> <Steve> Microsoft seems to be a constant target for hackers, why is that?
> <Kris> They seem to epitomize the anti-hacker mindset of, "Don't ask what's inside, just take our word for it, we know what's best for you." As a result, Microsoft represents conformity. It represents going with the herd. Hackers don't like to be told what they can and cannot do with THEIR toys. (interview)

***Principle #7: All Information Should be Free***

Consistent with the other principles of their ideology, hackers also believe that access to all (or most) information should be free and unrestricted. In particular, this belief ties in quite closely with the ideals of anti-authoritarianism and sharing knowledge. For hackers, the general view is that, in order to develop the best products (e.g., software, electronics), work efficiently and ultimately attain greater understandings, information that is of any worth to society should not be held back from individuals.

Freedom of information is a widely held belief within the hacker subculture. As a number of quotes in this chapter have already shown, hackers commonly reference this principle as one of the most central tenets of their philosophy. Some online hacker communities have made this principle explicit in their group's rules. Note the following rules posted on a hacker Bulletin Board System:

> Our rules here are simple:
>
> 1. Fnord.[27] Don't get Johnnie upset.
> 2. Respect the thoughts and opinions of others. No flame wars.

[27] Definition from "The Jargon File" (Raymond, 2000b): "fnord: n. ... A word used in email and news postings to tag utterances as surrealist mind-play or humor..."

3. **Promote the free exchange of knowledge and information.**
4. No illegal activity will be tolerated. No warez, codez or hackerz.
5. Don't panic. (BBS posting)

The hacker in the next dialogue maintains that the belief in the "free-flow of information" does not only apply to "computer knowledge" (e.g., Open Source software), but to all forms of information:

> <Steve> How would you characterize the hacker ideology or perspective?
> <Brad> The ideology, I'd say is the free-flow of information. That is common to most, if not all hackers...
> <Steve> I guess the free-flow of info would tie into things like open source software.
> <Brad> Not only software, but things like, "What is the government doing with a $50,000 hammer? What is NASA doing? What does company X have about me in its records?" All information. (interview)

Governments and corporations are often seen as holding the keys to a considerable amount of information and thus, hold significant control over people's lives. The information they possess may be anything from proprietary source code for computer programs all the way up to "top secret" details about military testing. Hackers believe that such information should be made known to the public for two main reasons. First, businesses and governments are not always seen as acting with people's best interests in mind. Second, unlimited access to information will allow bright individuals, such as hackers, to contribute to furthering the world's knowledge. Ultimately, the rationale behind this belief comes back to the hacker's wanting to know. For these reasons, professed

"ownership of information" is met with derision. Thus, copywriting, patenting and the development of proprietary software are also frowned upon.

Software development is a key activity, which hackers believe benefits from the free-flow and sharing of information. As such, hackers commonly advocate an open source coding system for software development, where the actual program code behind computer applications is made known to and built by a community of programmers. Open Source software such as the increasingly popular Linux operating system, are computer applications that are free and open to the public to contribute to its creation. The hacker in the following quote maintains that Open Source software, and more specifically, the philosophy behind its development (i.e., information should be free), is a key aspect of the hacker spirit:

> Also, you may want to check out Open Source software and its philosophy, which identifies absolutely with the "hacker spirit". I've never met a hacker who isn't all for open source software...(e-mail correspondence)

If more software was created under this model, hackers believe computer programs would be made better and that people wanting more control over their computer applications could have it. More so than an attempt to compete with mainstream software developers such as Microsoft, the underlying ideal is that all information should be public knowledge, shared, and available free (or next to free) of charge.

Some hackers take more of a moderate view on making information accessible. These individuals suggest that only certain types of information

should be made available, and then, possibly not to everyone. They also indicate that people sometimes take the Open Source concept too far. Note the following comments:

> <Matthew> I don't believe ALL knowledge should be free and shared. There is absolutely no reason to teach people how to build nuclear weapons with household supplies. And I do believe in closed-source software.
> <Steve> Why the necessity for closed-source software?
> <Matthew> The most important thing is balance - I appreciate software tools that are open source, I even use them - but the requirement to make a final software application open-source is ludicrous. End users do not need access to source. Nor should they be getting a free ride. It costs money to develop and maintain software. Source, even when closed, should be available for review when it deals with security, and sometimes even available for modification by the purchaser, but never required to be able to be used for another project entirely. (interview)

While freedom of information is very much part of the hacker perspective, the ways in which hackers apply this belief varies. Some hackers may be content to advocate their beliefs through Open Source software development, whereas those with a more malicious bent may take the "freedom of information" ideology to its extreme by engaging in malicious acts of computer intrusion to acquire access to information and advocate their ideals. Adhering to this perspective, some crackers resort to criminal measures to acquire information and rebel against large corporations and governments. The acquisition techniques and advocacy measures that these individuals take involve such things as the theft of program code, breaking into a company's network server, defacing government web pages, and spreading viruses through popular e-mail systems (such as the "I LOVE YOU!" virus that was spread through Microsoft's Outlook e-mail system).

## DISCUSSION

This chapter argued that there are seven core principles of the hacker spirit, which remain more or less consistent across the various subcategories and local subcultures of hackers. Each of these elements is premised on the overarching goal that one should strive to acquire an ever greater understanding of how things work. The principles of the hacker spirit include:

- *Principle #1: Higher understanding requires an unorthodox approach.* In order to reach a level of higher understanding, it is essential that a hacker take a creative approach to problem-solving.

- *Principle #2: Hacking involves hard work.* Along with taking a creative approach to problem-solving, a hacker must also realize that solving problems can be, and often is, hard work. Therefore, long hours of dedication to one's project(s) is essential. It was suggested that younger generations of hackers often lack this sort of concerted focus and thus, are critized for their laziness and misappropriating the hacker title.

- *Principle #3: Hacking requires a "learn for yourself" approach - learn by doing.* Problem-solving not only requires a great deal of ingenuity and hard work, but a hacker must also be self-motivated and seek to understand by taking a hands-on approach. Hackers suggest that you do not learn how to be a hacker, rather hacking is a way of thinking about and approaching a problem that cannot taught, but is self-directed and something that "comes from within." Novice hackers quickly learn to first attempt to solve problems on their own before seeking help from others. If you are able to show that you have done your own research, others will be more likely to assist you (depending on your project).

- *Principle #4: Share your knowledge and information with others.* In striving for ever greater levels of understanding, it is imperative that people share their solutions to problems so that other hackers can devote their time to new problems and build upon one another's findings. However, different groups have different informal protocols that one should follow when asking for information. Knowing the various actors within the hacker community, developing informal networks across the community and knowing what information the different groups covet, as well as the value (e.g., monetary, reputational, "pure" knowledge) they

place on their knowledge, are important to know when seeking out information.

- *Principle #5: You're evaluated based on what you know and your desire to learn.* Hackers indicate that physical appearance, degrees and style are inconsequential in the subculture. Instead, hackers' status and reputation are based upon their level of knowledge, creative self-directed problem-solving, and display of skill. Consequently, ignorance is highly disparaged. Some hackers suggest that this principle does not appear to be as important to the latest generation of "hackers."

- *Principle #6: Mistrust authority.* Hackers believe that people who hold positions of power within society, value and impose conformity, which hackers see as stifling creativity. Authority figures are also seen as not always acting in society's best interests. Therefore, hackers argue that these people are to be mistrusted and their attitudes challenged. Some hackers suggest that a document entitled, "The Hacker's Manifesto" exemplifies this principle and the hacker spirit in general. Although not all hackers agree with it, components of the Manifesto, such as its discussion of the misunderstood intellect of the hacker, is something that a number of hackers say they can relate to. Other hackers suggest that the Manifesto is misused by "impressionable" individuals to justify illegal behaviour.

- *Principle #7: All information should be free.* Hackers believe that information that is of any worth to society should be made available to everyone. In order to safeguard against abuses of information and assist in the furthering of knowledge, hackers maintain that ownership of information should be opposed. As an alternative, they advocate a model based upon the free-flow and sharing of knowledge. A pertinent example of information sharing is the development of Open Source software, to which a community of hackers contribute their programming efforts. Some hackers suggest that the *all information should be free* aspect of their ideology can be taken too far and that certain so-called hackers misuse the principle to justify inappropriate behaviour.

The hacker ethic, described by Levy in 1984, appears to still have a great deal of relevance to current generations of hackers. One significant difference, however, is the way in which the ideology is now being applied in light of "new" hacker activities.

It is important to note how the various "subcategories" or "types" of hackers use the ideology. Similar to the definitional issues discussed in the previous chapter, hackers draw boundaries between the different subgroups within the community in terms of how they apply their ideology. When expropriated to justify illegal behaviour such as copying proprietary software, within the subculture the person is more appropriately identified as a cracker or warez d00d, not a hacker. So while an outsider may identify hackers in terms of their endorsement of the subculture's ideological principles, hackers further distinguish between members of their community in terms of how fully they subscribe to the hacker spirit and how the ideology is applied to rationalize their activities.

The tenets of the ideology are used to counter prevailing perspectives and rationalize certain behaviours. In this sense, we can also see how the hacker ideology becomes used as a vocabulary of motive (Mills, 1940) for the different subgroups – i.e., a way of talking about hacking that justifies the behaviour. Although hackers incorporate aspects of the hacker spirit into their vocabulary, the different activities, which their ideology is used to justify, varies. For instance, while one group might draw upon the *all information should be free* tenet to rationalize defacing a "corrupt" government's web site, another group (or the same group at a different time) employs it to rationalize the communal development of Open Source software. For acts interpreted as deviant or criminal by outsiders, the use of the hacker ideology to rationalize these behaviours becomes a technique of neutralization. Thus, their ideology also functions as a

way of managing the stigma that both outsiders and certain insiders associate with particular types of hackers and their behaviours.

The hacker subculture also serves to normalize behaviours and perspectives that outsiders perceive as deviant. Given hackers' overlapping involvement in other subcultures (e.g., the student, family, sport communities) and outsiders' (e.g., media, government) portrayal of the hacker subculture, they are aware of outsiders' assessments of their behaviour and perspectives, and recognize that outsiders often see them as deviant. However, associating with others who adhere to a similar perspective, which is enacted within a more or less non-hostile setting, reinforces hackers' individual perspectives. To apply Cooley's (1922) notion of the "looking glass self", the community of hackers serves as a social mirror in which each individual hacker judges him or herself and the appropriateness of his or her accompanying perspectives and activities. Given that the hacker subculture provides a fairly consistent positive reflection of their perspective, one's perception of self, including the way in which he or she views the world, is supported and encouraged. Thus, the subculture acts as a culture of peer support and recognition in which people with similar viewpoints are accepted for adhering to the group's ideology. Behaviour and ideals that might otherwise be thought of as deviant are normalized within the context of subcultural interactions. This general argument is consistent with some of the propositions of Donald Sutherland's (1947) theory of *differential association* and Daniel Glaser's (1956) notion of *differential identification*, which have been

employed to explain the acquisition and internalization of norms and perspectives in various cultures. For instance, Simmons (1973) employs these ideas in his study of a group of mystics to describe how they are able to maintain a belief system that, for the most part, is contrary to most outsider perspectives:

> A further means by which the [mystic] is able to maintain his beliefs is through differential association and differential identification with [mystics] and relative insulation from non-[mystics]. As an interacting group, [mystics] provide support for the individual member in his view of the world. As a number of fringe group members have put it, they feel they can be themselves only with kindred fringers. Members feel they are "at home" because they share a common language with which they can communicate about their views and problems to alters who share their meanings. (p. 312)

However, inconsistent with Sutherland's theory in particular, the argument being made in this thesis is that, rather than being propelled along a certain pathway towards an ideology by *causal factors* (e.g., an excess of definitions in favour of violating the law), *how* individuals acquire perspectives has to do with their *interpretations* and the *choices* they make during the course of their negotiations and interactions with both insiders and outsiders.

An individual's own application of his or her perspective may not coincide with one group of hackers, but, given the diversity of the hacker subculture, it may fit quite closely with another. In the past, hackers were fairly isolated in terms of sharing their perspectives. With the advent of ever-greater network capabilities, new communication technologies such as the Internet, allow this once geographically disparate group to come together, choosing from a multiplicity of net-based communities, to share their thoughts and perspectives

with one another. The perceived anonymity offered by the Internet and its relative lack of censor permits for the interaction of individuals and sharing of perspectives in a way that was not possible, or at least much more difficult, during previous times.

Although the term "hacker" has, by and large, been attributed to computer hackers, hackers suggest that the concept can be applied to any individual who works hard at and takes delight in striving to understand how things work. As was noted in this chapter, one of the main characteristics of hackers is their "want to know and drive to learn" perspective. In a generic sense then, a person with this sort of mindset can be a hacker in any area of substantive interest, as long as it moves them to learn and create:

> The hacker mind-set is not confined to this software-hacker culture. There are people who apply the hacker attitude to other things, like electronics or music -- actually, you can find it at the highest levels of any science or art. Software hackers recognize these kindred spirits elsewhere and may call them "hackers" too -- and some claim that the hacker nature is really independent of the particular medium the hacker works in. (Raymond, 2000a)

No matter what the activity this perspective is being applied to, a hacker must necessarily be a person who thinks outside the box and seeks to move beyond our common or taken for granted understandings of the world. As another interviewee describes, doctors are a good example of hackers and the hacker approach to understanding:

> <Matthew> Doctors are really just medical hackers. They discovered much of what they know about the human body by breaking, picking it apart, and trying really silly ways of fixing it (bleeding one out to cure the flu, etc.). (interview)

As Taylor (2001) suggests, hackers think of hacking in terms of the unorthodox use of any artefact. Take for example the following comments:

> <Kris> I don't enjoy it [i.e., working with computers] as much as I used to. I'm bored with it. I do it out of habit. I'm finding my interests changing. I'm a lot more interested in metal working these days and gunsmithing...But I suppose that's the hacker mindset at work again; hackers abhor stagnation, and 18 years of my life doing one thing is exactly that. Computers are just a tool to do things. I'm changing tools basically. (interview)

Therefore, the tools an individual works with and seeks to understand may change, but if the ideology remains the same, the person remains true to the hacker ideology.

In this way, we can envision the hacker ideology as being generic. Although individuals working in other fields might not consider themselves to be hackers, it is likely the case that they are able to relate to various principles of the ideology as they go about their activities and seek to understand. Given that this more positive image of the hacker is in opposition to the more dominant mainstream portrayals of this subculture, both in terms of computer hackers' deviant and computer affiliated stereotypes, it is unlikely that others would consider "hacker" as an appropriate label for themselves or their perspective.

Related to this last point, it is also important to note that, by attributing their ideology to other non-hackers, hackers can also be seen as attempting to shed their negative public image. Rather than accepting outsider perceptions that the hacker perspective is somehow strange or deviant, by drawing parallels with other cultures, hackers promote their perspective as being normal and honourable.

By linking their perspective to others, especially those whom the public see in a favourable light (e.g., doctors, athletes, etc.), the use of such arguments acts as a further form of stigma management. Simply put, the imputed relationship serves as a claim of credibility. Merely by suggesting that the hacker mindset is not so much unique to their community, but is a perspective shared by other "normal" subcultures, they promote a more positive view of their own community.

The hacker ideology can be seen in the community's other subcultural characteristics such as its identity and activities. The vocabulary of the hacker subculture is no exception. In examining the unique linguistic characteristics of the hacker community – its argot – we are also able to observe evidence of the influence of the subculture's ideology. The next chapter examines the argot used by hackers in conveying their understandings about the world and, in so doing, employ and promote their ideology.

# CHAPTER SIX

# HACKER ARGOT

*The development and use of language is pivotal to the human accomplishment of intersubjectivity and group life as we know it. Denoting a shared symbolic system or a set of mutually acknowledged referents, language allows people to achieve life-worlds that are profoundly social and uniquely enabling (Prus, 1997, p. 89).*

## CONCEPTUALIZING ARGOT

The formation of culture is necessarily a linguistically mediated process (Prus, 1997). Without the capacity to exchange ideas through symbolic interchange, culture could not be shared, and therefore, people would be unable to formulate intersubjective understandings about the world. It is through language that individuals are able to achieve a "sense of mutuality" with others (Prus, 1997, p. 7). This, in turn, allows for culture to be passed from person-to-person, group-to-group and across generations. Dependent upon people's access to different communication channels, culture is dispersed beyond individual groups to the larger populace. Therefore, people are not only able to accumulate shared

understandings across time, but also across space.[28]

Although members of a society might have a pre-existing language in common, as they form groups around certain types of activities, they often develop a more specific vocabulary that may only be understandable to other subcultural insiders (Mitchell, 1983; Letkemann, 1973; Prus, 1997; Shibutani, 1955). Take for example Mitchell's (1983) ethnography on mountain climbers. In his research he found that climbers have developed their own set of expressions and a specialized language. These components of "mountaineer talk" develop as ways of expediently communicating consequential situations (e.g., falling rocks or climbers), identifying objects (e.g., various forms of snow, specialized equipment), associating with other climbers (e.g., greetings, stories), and denoting the importance of various aspects of the climbing experience (e.g., weather conditions, precarious situations).

Similarly, Letkemann's (1973) interview-based research on professional thieves (e.g., bank robbers, safe-crackers) points to the significance of a

---

[28] The centrality of language to the human capacity to found societies and develop culture is a point that was well-recognized thousands of years ago by the early Greeks:

> ...[N]ot only have we escaped the life of wild beasts, but we have come together and founded cities and made laws and invented arts; and, generally speaking, there is no institution devised by man which the power of speech has not helped us to establish...And, if there is need to speak in brief summary of this power, we shall find that none of the things which are done with intelligence take place without the help of speech, but that in all our actions as well as in all our thoughts speech is our guide, and is most employed by those who have the most wisdom. (Isocrates, 1928: 79-81)

As Prus (1997) argues, language is the most enabling invention of human creation. Given its centrality to the formation of human group life and culture, the ways in which people develop and employ language are points that merit the attentiveness and concentrated consideration of the ethnographer and social scientist more generally.

distinctive language – commonly referred to as a thieves' cant – for this particular subculture. Using a "work" analogy, Letkemann (1973) likens the criminal's approach to their activity as an occupation. In so doing, he offers an overview the various forms of "professional" jargon used by insiders. For instance, he notes that this group uses a number of terms to differentiate between subcategories or types of criminals (e.g., rounders, bums, young punks), describe techniques used to carry-out their work (e.g., loiding, peeling, shooting for space), and name the assorted tools of the trade (e.g., grease, knockers).

Related to the specialized vocabulary of a subculture are other linguistic characteristics that become part of the subculture. These characteristics can include, but are not limited to, different modes of communication (e.g., CB radio, cellular phone, Internet, sign language, letters), grammatical alterations (e.g., omitting punctuation, verb-doubling), and styles of speech (e.g., varied pronunciations, dialects, intonations, accents). As Prus (1997) notes, a subculture's more distinctive language may develop as a reflection of their: differing experiences (or challenges); developments in concepts and technologies; concerns with autonomy (and secrecy); or, interests in achieving particular communication contents (themes) (p. 69).

The human capacity to develop intersubjective "stocks of knowledge" and thus, shared perspectives and understandings of the world, is directly related to people's ability to communicate:

> As Dewey emphasized, society exists in and through communication; common perspectives – common cultures –

> emerge through participation in communication channels. It is through social participation that perspectives shared in a group are internalized. (Shibutani, 1955, p. 565)

Communication, or the sharing of symbols, is enabled primarily through linguistic interchange (i.e., speech and writing), but also occurs through the exchange of other forms of verbal (e.g., non-linguistic vocal gestures – moans, sighs, laughter) and non-verbal (e.g., physical gestures – sign language, facial expressions, body language) interchange.

As objects are assigned different meanings to account for their importance to a specific group, some groups develop a formal lexicon of subcultural vocabulary and idioms. In other subcultures the group's argot is ephemeral, existing only informally, and might not be entirely exclusive to a particular community. As a group's language evolves to formulate new ways of conceptualizing objects, their perspectives necessarily change to correspond with their "new" linguistic reality.

Meanings associated with certain words vary from subculture to subculture. For example, while grease and oil are commonly thought of as lubricating substances, among safecrackers the word takes on the additional meaning of nitroglycerine, which is used in the cracking of safes (Letkemann, 1973). Therefore, in entering into an unfamiliar community, newcomers will likely encounter new symbols and redefinitions of objects and activities that they had associated with other life-worlds (Prus, 1997, pp. 89-90). Part of the

involvement process for new group members then, will necessarily revolve around their ability to develop communicative fluency within the group.

The nuances of a new language may only truly be grasped through direct observation or participation within a group that speaks the language. Through this type of involvement people are better positioned to comprehend the experiential aspects of a language such as what words are used in what situations, how the meaning of a word changes based upon the context, the additional meaning given to expressions based upon insider jokes or stories, and even the inflection or intonation in one's voice which signify different meanings. It follows then that an outsider can only truly appreciate a subculture's argot by experiencing its use first hand. By examining how hackers employ language both on- and off-line, this chapter explores the distinctive linguistic aspects of their culture.

## THE HACKER LANGUAGE: TECHSPEAK AND JARGON

> *<Steve> You there Matt? I've been getting some weird disconnects.*
> *<Matthew> i can see that ... it's probably Bob's router*
> *<Matthew> ...again...*
> *<Steve> I thought Phil was running the show?*
> *<Matthew> Phil's box is at Bob's work ... behind Bob's isp's router, which is a piece of junk no one can do anything about*
> *<Matthew> actually, its not Bob's router's fault today. telus is having backbone problems*
> *<Steve> Oh really? How do you know that?*
> *<Matthew> tricks of the trade: "traceroute" between yourself and the server you are testing. Then ping-flood each connection in order until one of them starts losing packets "ping -c 100 -f" (that limits it to 100 packets in case the connection drops on you, and you can't hit CTRL-C to break the ping flood). (field notes)*

After reading the introductory quote to this section, a person who did not know I was communicating with Matt in Internet Relay Chat, and who was unfamiliar with the conventions of online communication and the technology-based aspects of the hacker language, would be hard-pressed to understand the conversation we were having. Without knowing that I was chatting with Matt over the Internet, you might first have been wondering, why am asking if Matt is there? Surely, if it were a face-to-face dialogue one would assume that I could visually determine Matt's presence. Knowing that the dialogue is a text-based chat, you might be asking yourself, is Matt a poor speller? Does he know proper grammar? Why does he not capitalize his 'I's or the first letter of each sentence? Why the ellipses? More likely though, questions regarding the technical terminology (if, in fact, specific terms were recognized as being technology-oriented) in the dialogue would be the most pressing. If you were aware that I was speaking with a hacker you might have assumed that words such as "router," "box," "backbone," "ping," "flood," and "packets" are being defined differently in this conversation than common understandings of these terms. Otherwise, you might be questioning, what does Bob's router have to do with being disconnected? Why does Bob have Phil's box at work? What's wrong with telus' backbone? What's being flooded? What's in the packets? Of course, greater contextualization would have provided essential information for understanding the conversation. Should I have premised the dialogue with a remark such as, "Continuation of Internet interview with hacker respondent 'Matthew'," you

would have at least been able to envision the transaction as an online chat and possibly expect the conversation to include some technical terminology. However, beyond me situating the conversation, you would necessarily have to be familiar with hacker vocabulary or, at the very least, computer and network terminology to grasp the dialogue's substantive content. There are many aspects of the opening quote that are difficult to understand – *as a hacker might understand them* – if you are not versed in the subcultural argot of the hacker community.

Hackers not only pride themselves for being technologically creative, but also take delight in employing creative linguistics. Immersion within the community leads to one developing associations with others who are at different points in the process of not only acquiring but also developing new vocabulary and styles of speech. The use of the group's argot becomes commonplace, so much so, one informant notes, "I don't really recognize it anymore. It's part of my everyday language" (interview). To those not versed in the particulars of hacker argot, engaging hackers in discussions about their activities or even sitting back, listening to and trying to understand their conversations can be a difficult task. As I observed after one of my meetings, if you are an outsider to the hacker subculture or are unfamiliar with science fiction and technical terminology, it is very difficult to penetrate their conversations and understand what they are discussing:

> When it came to a lot of the electronic stuff, for the most part, I had really no clue what they were looking at and what they were

> talking about when they discussed its uses. When I asked them to explain it to me, they ended up using words that I didn't understand anyway...Mark and Terry in particular seemed to be very knowledgeable about the inner workings of electronics, but even this was hard to discern because of my lack of knowledge in the area. For as much as I know, they could have been totally wrong and making things up. (field notes)

Even before meeting with hackers I was sceptical of an outsider's ability to comprehend their discussions:

> From what I've read on their web pages, hackers have a jargon of their own. Add that to the technical nature of their activity - i.e., computer programming and electronic "manipulation" - and my limited understanding of terms may make it difficult for me to communicate on the same level as them. I recognize this as a boundary to any endeavour into an unknown subculture, where one has to be re-socialized to the new culture. (field notes)

During one of my meetings I shared my scepticism with Jerry, but he assured me that understanding the hacker language just takes time and that it is a learning process that all newcomers go through:

> I told Jerry that all I really could do was observe because a lot of the stuff was just going right over my head. He said that after a couple of months of listening you get to know the lingo - the hacker language as he referred to it. (field notes)

It follows then that a key aspect of becoming initiated into the hacker community is developing communicative fluency with the insider language – i.e., learning, adopting and using the group's argot.

The following sections explore the terminology used by hackers, which sets their language apart from other cultures. In particular, the various jargon and "techspeak" of the hacker subculture are what make up its argot. There are some

significant differences between jargon and techspeak, which are explored in the following sections.

**Techspeak**

Techspeak is the formal technical language of hackers. Raymond (2000b) indicates that techspeak involves standard computer terms (e.g., Operating System, megabytes, Interrupt Requests, ports), which appear in textbooks, technical dictionaries, and other technology-oriented manuals. The technical vocabulary of the hacker language is not so much unique to hackers rather it is typically used by people in programming, computer science, electronics, and related fields of study and employment (Raymond, 2000b). This point was reiterated by some of the hackers I spoke with. For example, as the hacker in the next interview excerpt indicates, Techspeak tends to be used by "techies" more generally:

> <Steve> ...Now there's a lot of computer terminology that goes on too, that's probably not exclusive to hackers...
> <Shawn> No, that's just techie stuff. If there's anything that doesn't make sense, feel free to ask for clarification, we usually don't know when we're speaking another language. (interview)

Shawn's comments also reinforce a point made in the last section. That is, the use of such technical terminology becomes commonplace for hackers. They become so used to using these terms, that they often take for granted that others present during their technical discussions are also familiar with the terminology. Given that they are presumably in the presence of other hackers, this assumption is well founded.

Communicating with other hackers who share a similar language permits for a mutual set of unique symbols that convey the meanings specific to the objects of interest to them. In order to achieve mutual understanding though, the meanings attached to the symbols must be shared.

As the introductory section of this chapter revealed, the hacker culture is not unique in its formation of a distinctive language. As the following hacker's comments indicate, each life-world that is formed around a specific activity, with a unique set of objects and rituals (or different meanings for objects and rituals than what an outsider may have), often develops a technical argot:

> <Steve> Is there a certain hacker language, jargon or terms that one has to be familiar with in order to understand what's going on or what people are talking about?
> <Matthew> ...I know I am hitting on this a lot, but it really is no different than a group of musicians talking about reeds, keys, pads, decks, soundboards and the like. (interview)

The next hacker's comments also pick up on this point by suggesting that the use of a technical vocabulary helps individuals to better express their ideas. He says:

> <Brad> ...like doctors use a certain language when talking to each other, so do hackers. Things like routers, gateways, source code, it makes the technical ideas easier to express. Slang, jargon, etc. most people can pick up pretty quick... [There's] words like w00t, lol, brb -- a lot come from IRC/MUDs [Multi-User Dungeons – virtually mediated online role-playing worlds]. But in general, a complete newbie, minus the technical terms, which you're going to have to learn if you want to be a hacker, and not a cracker, the jargon/slang is like any other group, listen for a while, and you'll understand most of it. (interview)

Brad's comments raise a number of relevant points regarding argot and its use by hackers. First, a specific technical vocabulary allows hackers to better

conceptualize objects of interest to them and communicate their ideas more precisely. Second, he discusses the adoption of terminology used by hackers online as being developed by people's overlapping participation and sharing of ideas through their involvement in other Internet-mediated communities. Third, he points to a difference in the level of knowledge and the related vocabulary, which differentiates hackers from crackers. For Brad, a hacker is a person who knows the technical terminology of the culture because he is very knowledgeable about the use of computers. A cracker, on the other hand, is seen as being less knowledgeable about computers and therefore, not as likely to need or employ the technical language. Finally, he points out that someone new to the culture can begin to understand the hacker language by listening to how it is used by other hackers.

Throughout the interview and the participant observation components of this research, it became obvious that a layman's understanding of computers (and related technologies) would not suffice in this community. If one wishes to understand and participate in hackers' discussions, especially when they are speaking specifically about computers and programming, one has to be well versed in the related technical vocabulary. As the hacker in the next interview excerpt explains, a base level of knowledge about computers and networking is essential. Beyond that, an outsider may be able to supplement their understanding of the interactions through observation and probing for explanations:

> <Steve> Is there a certain hacker language, jargon or terms that one has to be familiar with in order to understand what's going on or what people are talking about?
> <Rick> Well, there are LOTS. The baseline is to know the terms used with computers and networking in general. Which covers a LOT of things. Most of the rest of the jargon can be figured out with common sense usually, or by asking someone "Hey, what does that mean?" You'll be able to figure it out. (interview)

Similarly, the hacker in the next dialogue indicates that, while it is impossible to be familiar with everything other hackers will discuss (as they have varied interests and areas of expertise), it is necessary to develop a base level of technical vocabulary and be familiar with computer-related technology. Beyond that, she notes that it is impossible to be familiar with all the technical vocabulary. She suggest that there are simply too many areas of technology to be aware of, which are evolving quite rapidly, thus making it impossible to keep pace:

> <Steve> Is there a certain hacker language, jargon or terms that one has to be familiar with in order to understand what's going on or what people are talking about?
> <Andy> Not really, I mean, if you don't know Unix, or you've never seen the inside of a computer, you're likely to get lost in a technical discussion. It's all a matter of what's being discussed at the moment. It's impossible to know everything about everything. There is simply too much to keep up with. I'm trying to catch up on ipv6 right now, because I got lost the other day in a chat, heh.
> <Steve> So a lot of technical talk?
> <Andy> Of course, we're computer geeks, after all ;-) (interview)

By being able to dialogue on the same level as others in the community, hackers are able to share in the group's ideas. While variants of terminology exist, there is still enough common ground between hackers that shared understandings of technical ideas are able to transcend the different groups.

**Jargon**

Jargon is the slang of the hacker language. While the various terms which make up the hacker jargon may eventually become part of techspeak (i.e., become formalized in dictionaries and manuals), they usually remain at the level of informal usage and often do not relate to technology. Hacker jargon has an extensive history dating back to the early days of the culture at the MIT labs (Raymond, 2000b). In fact, hacker jargon appears to be one of the most developed traditions of the subculture. Take for example the 450 plus page "Jargon File." The Jargon File is somewhat of an informal dictionary of the hacker language, defining not only the "established" jargon of the subculture, but also describing jargon construction procedures and the reasoning behind these techniques. The first version of the Jargon File was developed as a collaborative initiative from 1973 to 1975 (Raymond, 2000b). Like any language, not all forms of jargon are frequently employed by the subculture. Some groups extensively use hacker jargon, while others mix in the odd term with techspeak and the English language. Still others develop their own unique terminology to reflect such things as the insider jokes, interests, events and activities of their particular group.

What follows is a discussion of the various forms of jargon commonly used by hackers as observed during the fieldwork and interview portions of the

thesis research. Some of these different forms of jargon include: (a) Netspeak and conventions of online communication; (b) 31337SP34K; and, (c) role labels.[29]

### *Netspeak and the Conventions of Online Talk*

There are various forms of online vocabulary, commonly referred to as Netspeak, which have been in more or less constant development and use since people began using the Internet (and networked computers more generally). Although hackers have played a significant role in formulating this form of online jargon, most adept "netizens"[30] are familiar with at least the basics of Netspeak. There are slight variations in Netspeak from one online communication medium to the next. I will focus on Internet Relay Chat (IRC) in this section, as it was the primary communication medium through which I interacted with hackers while online.

One hacker points out, "...we [hackers] tend to abbreviate a lot. We use our own slang, our grammar sucks and so does our spelling (see my repeated use of 'cuz' in place of because)" (interview). Another interviewee suggests that he is convinced that much of what is distinctive about hackers' online vocabulary is a result of "lazy typing" and "honest typos" (interview). Written mistakes and abbreviations are quite common in real-time chats as there is a general consensus that people should try to communicate as efficiently as possible. This often

[29] These three categories of hacker jargon are by no means exhaustive, however, they do represent some of the most common aspects of hacker jargon observed and discussed during the research for this thesis. For an extensive glossary of hacker slang I recommend turning to "The Jargon File" (Raymond, 2002b).

[30] "Netizen" is Netspeak for Internet Citizen.

means not taking the time to write-out full words, phrases and sentences and not correcting spelling and grammatical errors. To simulate real-time conversations, IRC chats (and other forms of instant messaging such as ICQ and Microsoft Messenger) tend to include more short forms (e.g., w = with, y = yes, n = no, a/s/l = age/sex/location, ppl = people) and acronyms (e.g., lol = laugh out loud, btw = by the way, np = no problem) and a greater frequency of all lowercase messaging (e.g., "and mr. smith is my teacher for cs") and typos (e.g., "wher are we gong?") than other text-based asynchronous (i.e., delayed response) messaging (e.g., e-mail, newsgroup postings). As a result, for those unfamiliar with this aspect of the hacker argot, real-time chats can be reasonably complicated to decipher.

Instant or real-time messaging requires that online users be able to follow the often-complicated flow of conversation. Given the time interval between receiving, reading, interpreting, writing and sending a message, the ordering of messages in an online conversation can be difficult to follow. Furthermore, when there are more than two parties simultaneously engaged in an IRC chat it can be difficult to determine who is speaking with whom. Note the disjuncture in the following IRC conversation on the left and then compare it to my interpretation on the right (see Table 1):

Table 1. IRC Chat "Translated"

| *IRC chat as it occurred:* | *My interpretation of the chat:* |
|---|---|
| * Ted is confused<br><Marcus> heya Ted!<br><Sean> I'm seriously thinking of eating out this evening tho<br><Sean> Ted: about what?<br><Ted> heya Marcus<br><Marcus> how was your day<br><Ted> how are you today?<br><Ted> it was alright, pretty boring<br><Marcus> i am alright<br><Marcus> hold on a sec<br>* Ted thought that said, hold on sex<br>*** Morgan has quit IRC (Quit: )<br><Marcus> Ted can't read?<br><Daniel> back to work i go.<br><Daniel> byebye<br><Marcus> later Daniel<br><Sean> bye Daniel<br>*** Daniel has quit IRC (Quit: )<br><Ted> yeah, but my mind wanders<br><Ken> Sean how much did you pay for the floppy? and did you try futureshop or any of the stores on king?<br><Marcus> mine too<br><Sean> Ken: I bought a box and I dunno how much...king? guy, I'm in Dunnsville :b<br><Ken> so?<br><Ted> Marcus, you missed a fun night last night<br><Ken> should have though about it while you were in queensville :P<br><Marcus> really?what made it so much fun<br><Sean> I didn't need it while I was in queensville :b<br><Ken> suuurreee ;)<br><Ted> i was there :-)<br><Sean> heh | * Ted tells the people in the IRC channel he is confused<br><Sean> About what, Ted?<br>*(Ted does not respond to the question)*<br><br><Sean> I'm seriously thinking of eating out this evening though.<br>*(No one responds to Sean's comment)*<br><br><Marcus> Hey, Ted!<br><Ted> Hey, Marcus.<br><Marcus> How was your day?<br><Ted> It was all right, but pretty boring.<br><Ted> How are you today?<br><Marcus> I am all right.<br><Marcus> Hold on a second.<br>* Ted indicates that he thought that Marcus said, "hold on sex."<br><Marcus> Can't you read Ted?<br><Ted> Yeah, but my mind wanders.<br><Marcus> Mine too.<br><Ted> Marcus, you missed a fun night last night.<br><Marcus> Really? What made it so much fun?<br><Ted> It was fun because I was there *(Ted says with a smile).*<br><br>*** Morgan has quit IRC<br><br><Daniel> Back to work I go. Bye-bye.<br><Marcus> Later, Daniel.<br><Sean> Bye, Daniel.<br><br>*** Daniel has quit IRC<br><br><Ken> Sean, how much did you pay for the floppy drive for your computer? And, did you try Futureshop or any of the stores on King Street?<br><Sean> Ken, I bought a computer and I don't know how much it was for the floppy drive. King street, in Queensville? Guy, I'm in Dunnsville *(Sean says with a smirk)*<br><Ken> So? You should have bought it while you were in Queensville *(Ken says with a smirk).*<br><Sean> I didn't need it while I was in Queensville *(Sean says with a smirk).*<br><Ken> Suuure *(Ken says with a wink).*<br>*Sean laughs* |

As can be seen in this example, the flow and thus, one's understanding of each comment and conversation, is hampered by people interjecting comments into an ongoing dialogue, by individuals entering and leaving the chat room, and by overlapping discussions.

While the distinctive aspects of the hacker argot and online talk mentioned thus far may be a problem for an outsider, most insiders have acquired a sense of what the various short forms and abbreviations mean and acknowledge that others will take shortcuts and not always backtrack to correct mistakes so that real-time dialogue occurs efficiently. Of course, if it becomes obvious that people do not understand what someone else is saying, they will ask for clarification. This is accomplished through a process of (re-)definition and explication. For instance, I found it necessary at the begin of the online interviews to situate the discussion, define the meaning behind some of the symbols I would be using, and provide some indication as to how the respondent should interpret my lack of response to his or her answers:

> <Steve> The objective of the study is to learn more about certain characteristics of the hacker culture, as defined by participants. Some of the main characteristics of interest include common patterns of activity, ideology, language, identity, norms, and objects or artefacts. I'm also interested in examining how people become involved in the hacker culture. For this, it is necessary to speak with people who consider themselves to be part of the culture and have them share their perspectives with me.
> <Steve> Please keep in mind that I'm interested in your experiences. Quite often I will ask you to give me an example/instance of what you are talking about.
> <Steve> The key to this research is having those in the culture share their perspectives and experiences. Please be straight and up-front, there's no judging that goes on here. I will be using

information you give in my research paper, but everything will remain confidential as all your comments will remain anonymous. If you don't want to answer a question just tell me "next question."
<Steve> If I cut you off at any point (i.e., sometimes I might interpret a pause as you anticipating the next question) please continue with what you were saying and I will ask the question after you are finished.
<Steve> If you plan to continue on with a train of thought just use an ellipsis...
<Steve> If you see me pause too long, that may mean I'm thinking that you have something else to say. Just say "done" if you're finished what you have to say (e.g., for a big paragraph).
<Bruce> ellipsis?
<Steve> ellipsis = ...
<Bruce> Doh!
<Bruce> okay
<Steve> hehe... just need these little conventions to help the chat go smoother ;)
<Bruce> It's standard. I use them all the time... just like that even...
<Steve> hehe (interview)

As mentioned, during real-time IRC conversations there is a certain level of expectation that each party in the conversation will respond to a message in a reasonably short period of time. That is unless people indicate in some way to others in the chat room that they will not be able to reply forthwith. To do this, people use Netspeak conventions, which notify others of their online status. In IRC this is done by setting your "away status" or changing your pseudonym to reflect your availability. For example, a person calling himself "Dave" in IRC might change his nickname to "Dave[away]" to let others know he is away from his computer and likely will not be immediately responding to any messages. Alternatively, people will simply indicate to others in the chat room that they are going to be away from their computer for a bit. They might say, "I'm afk for 10"

(I'll be away from my keyboard for 10 minutes), "brb" (be right back) or "bbiab" (be back in a bit). Another indication that a person might not respond to a message in IRC is if their "idle status" indicates they have been idle (i.e., they have not sent any messages) for a significant period of time. An idle message such as "Dave has been idle for: 6 hrs 18 mins 5 secs" would suggest that Dave has his computer on, but might not respond to messages as he is likely away from his computer or busy doing something else on his computer.

As there are fewer ways to contextualize a message (e.g., through intonation in the voice, hand gestures, facial movements) via text-based communication, determining the meaning behind online messages becomes somewhat more difficult. Instead of relying on face-to-face cues, Internet-based text communication forces those interpreting messages to rely on fewer symbols from which meaning can be interpreted. In an attempt to compensate for this technical shortcoming, individuals add symbols and preface their responses to demarcate intention.

The most common set of symbols used to denote intention, and more specifically, emotionality, are what are known as "emoticons" (emotion icons). There are many different emoticons used online and they appear as both keyboard-based character symbols (e.g., :-) or :) = happy, :-( = sad, :-O = shock) and, more recently, graphical images (e.g.,  = happy,  = sad,  = shock), which can be added to some forms of online messaging. Note the extra meaning added by the emoticons in the following dialogue:

> <Rick> It appears as though Steve has a low self esteem. Why you may ask? The lack of capitalization on your name represents such a conclusion. Either that or his pinkie fingers have been cut off, and he can't use the caps. ;) ...
> <steve> Haha. I think it was just me quickly typing my name... hmmm... or was it? Now I'm going to have to pull out my psych books.
> <Rick> Sure, sure. Freud would have something to say about that. Especially in a person whom uses the computer often, the difference between hitting the shift button, and not hitting it becomes a subconscious issue in some. I would hypothesise that the case is as such here.. lol..
> <steve> Okay... I looked it up, Freud never wrote on typed communication. Ha!
> <Rick> You are correct Steve.
> <steve> Yes.
> <Rick> But neo-Freudians have. ;)
> <steve> Nooo!!!! (field notes)

Although it is likely clear from what Rick was saying that he was joking around with me, his use of emoticons reinforces his intention.

Along with emoticons, hackers use other symbols to denote particular virtual actions and will cordon-off phrases with words that are meant to add intention to their remarks, which, in turn, add further meaning to the conversation. This is done by surrounding or prefacing a word or phrase with an asterisk(s) or less than and greater than signs. Note the following examples:

> * Bailey chuckles (field notes)
>
> <Andy> *cough* mr.icreatedhacking *cough* (interview)
>
> <Matthew> <sarcasm> Now I'm really afraid! </sarcasm> (interview)

For those familiar with programming, and more specifically web page design, Matthew's use of "XHTML tags" (i.e., <sarcasm> </sarcasm>) adds another layer

of meaning to the discussion. Using programming code in such an opportune manner during one's online chats may be seen as a witty, inventive use of language. Without the use of emoticons and other symbols to convey intention and set the tone of the conversation, it is easy to misinterpret someone else's comments.

Beyond such manifest intention conveying symbols, people must rely on their understanding of the context of the conversation and the person who is communicating to determine the meaning behind the message. In order to develop a more complete sense of shared understanding – i.e., intersubjectivity, newcomers often have to move beyond dictionaries and their own interpretation of the conversation (which may be informed by previous experiences to a lesser or greater extent), and have others take the time to convey what a certain term means or how one should interpret a specific comment. In the informal interactions of everyday life, it is seldom the case though, that this sort of direct tutelage takes place. Rather, like any new aspect of language, it is through the experiential development of argot that hackers come to understand the meaning behind the various jargon and witness and learn the different ways in which people in different groups and contexts use particular words. The relativity of words and the meaning they convey must be interpreted based on the context, while taking into consideration the person conveying the message, as well as any interpretation cues he or she might offer.

***l3375p34k***

One rather common and contentious style of the hacker argot is what is known as l3375p34k. l3375p34k can be translated as Elitespeak or simply Leet for short:

> <Max> elite = eleet = leet = l33t. (interview)

Leet involves the substitution of numbers, other non-alphabetical characters (e.g., §, /, +, &, Ω), and combinations of these symbols (e.g., ><, {}, '//) for letters or groups of letters. Sometimes a number is used to represent the sound of a group of letters:

> <Cory> Then there's l8er...Or m8 is mate. 8 sounds like ate I guess. L-ate-r. l-8-r. (interview)

Other times, numbers and other non-alphabetical symbols are substituted for the letters that they resemble. Take for instance the following two examples:

> 0nly t#en '//!11 j00 +ruly b '337! (StankDawg, 2002, p. 41)[31]

> <Steve> I've been seeing a lot of writing in this style: "AAS ICAN AT LEaST ADMIT...lame i 4lso underst4mnd", what's the significance of it? Why the numbers and seemingly random caps?
> <Max> Well the numbers are meant to look like letters, it was a thing in the 80's that people would do, if you look at my handle '14rry-ph33r' it means 'Larry-fear' (3 = E and 4 = a and l or i = 1) dunno about the random caps that's just lameness?! (interview)

As Max indicates, hackers usually see the overuse of capital letters as being "lame." Lame is used frequently in the subculture as a derogatory statement. The term "lamer" is reserved for those people who have poor communication style and those with very little hacking skill who feed off other people's work to crack

[31] This line of Leet can be translated as, "Only then will you truly be elite!"

computers (Raymond, 2000b). In this way we begin to see how the use of certain words and communication styles get used by members of the hacker community to identify individuals and distinguish them as particular "types."

One hacker indicates that Leet is used, "...so that other people don't understand what they're saying" (interview). Similarly, another hacker states:

> <Cory> It's like code. Some people won't have a fucking clue what you mean and write it off. Or they will try and decipher it and since there is no code they won't get shit. (interview)

Beyond Leet (and possibly being confused with Leet), other types of "coded" communication exist in the hacker culture. As with Leet, such coded messages might be seen as an attempt to maintain a level of secrecy around what is being discussed. Two forms of code that were observed included real-time encrypted messages and the use of Binary[32] to write messages. Note the following two field note passages. In the first excerpt the two hackers are sending encrypted messages to one another:

> <Mike> (CRYPT:0) eXk.S/tvN6i10fZ/P0KpgYp1
> <Mike> hehehe
> <Bailey> (CRYPT:0)
> 1gFXt.YY1om0vwFQK.7Gfss.TbsV91pFCzU1M2g100kpcYm.
> <Mike> (CRYPT:0)
> jZnqX0hPpm10Mupgu/k177N.hM6Tx.kvB8G.
> <Steve> what was that?
> <Bailey> (CRYPT:0) 0FQ3e/QGDf60
> <Mike> It's encrypted, heh.
> * Bailey giggles
> <Mike> A little script I wrote. (field notes)

[32] Used by computers and other electronic devices, Binary is a series of ones and zeros, which relate to on and off electrical impulses.

In this next excerpt people are trying to read Binary messages posted by one of the people in the channel:

> <Dan> 01000100010001010100011001000011010011110100111
> <Dan> Read that. What does it say?
> <Tanya> 4 or 8 bit chars?
> <Tanya> 01000100 00100010 10100011 00100001 10100111 10100111 68, 34, 163, 33, 167, 167
> <Tanya> D"ú!ºº +
> <Tanya> D"ú!ºº ?
> <Tanya> What is that supposed to mean? C'mon I just converted Binary to decimal to ASCII for ya? What is a D"ú!ºº ?
> <Dan> No, just straight to ASCII.
> <Tanya> 01000100010001010100011001000011010011110100111. I miscounted the places. Only 47. You're missing a digit... Admit it, it's BS or tell me the purpose behind your 47 bit binary jargon. =)
> <Steve> What are they doing with the ASCII?
> <Dan> They're trying to read binary, but they're screwing it up... She is trying to use math. She needs to just do the straight ASCII conversion. (field notes / interview)

While these forms of code might be used for covert conversations, creating a program to write encrypted messages and being able to read and write Binary demonstrate a certain level of computer knowledge. There is also a significant degree of entertainment, enjoyment and challenge derived from speaking in and deciphering code.

In an article entitled, "A History of '31337SP34K'" a hacker using the pseudonym StankDawg (2002), describes that Leet became established during the early days of newsgroups. It was used as a way to get around newsgroup administrators who would use filters to delete objectionable material from their servers. He argues that:

> Since "hacking" fell under the "objectionable material" category, we had to intentionally misspell the word to avoid getting kill-filed.[33] OK, so they [i.e., administrators] add "hakker" to their filter. But what about "H4ck3r," "H4kk3r," "Hax0r," and so on? We kept adapting the language (and don't think this is any less of a language than Ebonics) until the censors finally gave up. We could make every word adapt and change to avoid being blocked. (2002, p. 40)

As StankDawg (2002) indicates, Leet is constantly being adapted and there are often many variations of a single word, thus making it hard for outsiders to read and computer filters to censor.

Although some hackers use Leet, people interviewed for this thesis described it as "a pain to read", "annoying to type", "lame", and "laughable." One informant indicates that Leet is only used by "real" hackers with heavy sarcasm to make fun of those people who think they are hackers because they talk using Leet:

> <Shawn> It's old, most people grow out of it, and just use it to emulate the "punk kids" of the hacking (h4x0r) world. (interview)

Similarly, other hackers suggest that Leet is only used jokingly or is used to deride others who call themselves hackers:

> <Kris> the big myth is that w3 4lL t4lK l1k3 tH1s. It's more of an inside joke that we perpetuate to the uninformed that we talk like that. (interview)

> <Max> [Leet is] a bit of a joke really, well I hope it is. (interview)

> <Rick> ...usually when someone is talking like that [using Leet] either they're making a joke, or they're what we refer to as "script

[33] A kill-file is an electronic file, which has a list of words and phrases that a computer program will look for in articles being posted to a newsgroup. If the preset text is found in the article, the article will not be posted to the newsgroup.

> kiddies" or people that really don't know much, but think they're the best. (interview)
>
> <Mike> Now I think leet speak is kind of used mostly as a joke. (interview)

Given how certain hacker groups see the use of Leet, interviewees advised that this form of jargon should be used sparingly and appropriately (i.e., as a joke) so as to avoid ridicule and possibly being stigmatized as a "script kiddy" or "newbie."

While "wannabe" hackers are now criticized for using Leet, some informants who are familiar with Leet's history pointed out that it once had its place, but has now been bastardized and overused. One hacker explains that Leet has become laughable because it is "primitive" compared to how it was once used. He goes on to describe that, in his view, the idea behind Leet was to be creative and show that you were knowledgeable about the more latent textual capabilities of computers:

> <Matthew> 1337 speak makes me laugh because it has become so primitive compared to the (British pound)(sigma)(sigma)(drawchar-top-centre) speak we used to use on BBS systems. (By the way, my IRC won't allow the real characters in here, so I had to give you the next best thing). MS-DOS supports 255 characters, and we used nearly 200 of them for variations of leetspeak.
> <Steve> What was the idea behind leetspeak?
> <Matthew> Creativity. It started using extended characters in signatures to show that you even knew they existed. (find an old MS-DOS computer, hold down the alt key, and type 157 on the numeric keypad to get one of them ... the yen symbol I think). Many people added ANSI colour codes to them - drawing mini-pictures. (interview)

Raymond (2000b) indicates that the term "elite" came into use in the hacker culture in the early 1980s. It was reserved for those hackers who were given access to the "hidden" or "privileged" sections of Bulletin Board Systems (BBSs). Matthew indicates that during the BBS era of the 1980s "elite" was mainly used as a label for "rippers" and "couriers." These people were held in high regard in the hacker community for transporting software programs, files and games across BBSs and making it possible for others to copy commercial software:

> <Steve> I have been told that leet can be read as elite, is that true?
> <Matthew> Yes. That takes me back. "Elite" was the original word used to distinguish normal users from the chosen few. Generally, it was the couriers and rippers that were "elite" back then. Couriers were the people who formed networks to transport files across the country without getting long distance bills. Hence the "Hayes Courier" 14.4, 16.8, and 19.2 modems with HS compression. They allowed full bi-directional transfers, so you could be uploading and downloading full speed at the same time - very useful when you sit in the middle of a courier network. This is back in the days of "0-day warez"[34] - except anything under 7-day was considered an exceptionally well connected BBS... Rippers are the ones who removed copy protection schemes. (interview)

Hackers who were considered "elite" were often those who were the most knowledgeable about computers and thus aware of the computer's capabilities to produce a set of somewhat hidden characters. They were also the ones who had the most interest in avoiding the filtering software that would be used to censor their discussions. Thus, these individuals were the ones who began altering the

[34] 0-day warez is slang for a software program that is "cracked" and distributed on the same day it retails.

characters in their words, a style of jargon that became known as elitespeak or 71337SP34K.

While the hackers whom I spoke with are somewhat more proud of the historical use and development of Leet, the point that particularly bothers them is that a person no longer has to be "elite" to use today's version of Leet. Add current "wannabe" hackers' lack of appreciation for the history of Leet's development (and the hacker community and its ideology and norms more generally), their belief that speaking in Leet will make others think they are hackers, and the more recent alterations of Leet,[35] and it becomes comprehensible how those considering themselves to be "true" hackers are irritated by the latest generation of "hackers."

Picking up on this last point, Raymond (2000b) argues that the frequent substitution of letters for numbers (e.g., 53nd m3 f1135 = send me files), abbreviated wording (e.g., u r supa c00l! = You are super cool!), and intentionally misspelled words (e.g., phreaks = phone + freak), are often overused and typically only employed by the underclass of the hacker subculture (e.g., script kiddies, wannabes, warez d00dz, warez kiddies, leechers). He contends that the closest that a "true" hacker will get to such usage is the switching of the dollar sign for "s" in the names of companies whose services are felt to be overly expensive and who are seen as being solely interested in their financial bottom line (e.g., Compu$erve, Micro$oft). The intentional misspelling of words, blatant

[35] For example, writing sentences in mixed case to make it look like traditional Leet = hERe i aM (see StankDawg, 2002).

grammatical errors, and other forms of wordplay may also be related to the counter-culture/anti-authoritarian attitude of hackers. Such misuse expresses unconcealed disrespect for the conventions of proper English and show contempt towards those who are seen as pushing society to conform.

As can be observed from the examples of quotes from hackers, a great deal of the creativity in their language can only be appreciated through observation of their written text. For example, the pronunciation of words such as d00d, warez, and ph33r are the same as their English language counterparts – dude, wares, and fear. An interviewee explains, "...hax0r means hacker, if you say it, it should sound the same." However, a number of hackers will make fun of someone who does not use the term in a satirical sense. For example, one respondent explains that his group uses the term hax0r as: "...a derogatory term to describe someone or a group who are pretending to be hackers" (interview). To denote sarcasm, some hackers will pronounce "hax0r" phonetically, just as it appears: h'ax'or. Aside from this use of rhetoric, which transpires as hackers attempt to draw lines between "real" and "false" hackers, the general point not to be lost is that hearing a certain word such as "Microsoft" does not convey the same meaning as it does when observed by the reader: "Micro$oft." This seems fitting as a great deal of hacker-to-hacker communication takes place via the Internet in textual format.

***Role Labels***

As was discussed in the chapter on definition, hackers use a number of labels to distinguish between the various actors in their subculture. Some labels such as "script kiddy", "warez d00d", and "leecher" are specific to the hacker subculture, whereas other labels are adopted from other subcultures and take on new meaning or are given further meaning in the context of the hacker community (e.g., guru, wizard, newbie, cracker, worm). Some role labels are simply attached to individuals to denote a particular area of expertise. Two good examples of this are the aforementioned "couriers" and "rippers" who were responsible for transporting files across BBSs and developing ways to defeat software copyright schemes. Other role labels are more value-laden and are used to laud or denigrate other members of the "hacker" community. For instance, being referred to as a "guru" or "wizard" represents particularly high praise for one's hacking ability. At the other end of the labelling spectrum, being called a "newbie", "script kiddy", "lamer", "leech" or "warez d00d" tends to denote a low level of hacker knowledge and signify one's relative immaturity regarding what it takes to be a hacker. The name, "troll" is given to those people on newsgroups and in chat channels who are solely interested in or become known for disrupting a group's communication. A person who frequently "flames" other people within the newsgroup or chat room is often referred to as a troll. Therefore, hackers indicate that they may avoid using newsgroups as they are "overrun by trolls and kiddies" (interview) and develop rules about how to avoid instigating a troll:

> <Andy> Don't feed the trolls... easy as that... didn't your mother ever teach you that those people are just out for attention? (interview)

These few examples are just a small sample of the various role labels used within the hacker community.

Certain role labels are based on elements of hacker folklore, both real and mythical, which are comprised of insider jokes, stories, and events. For instance, in "The Jargon File", Raymond (2000b) describes the fictional hackers, B1FF and Jeff K., whom hackers use to refer to prototypical "newbie" or "wannabe" hackers:

> :B1FF: /bif/ [Usenet] (alt. `BIFF') n. The most famous {pseudo}, and the prototypical {newbie}. Articles from B1FF feature all uppercase letters sprinkled liberally with bangs, typos, `cute' misspellings (EVRY BUDY LUVS GOOD OLD BIFF CUZ HE"S A K00L DOOD AN HE RITES REEL AWESUM THINGZ IN CAPITULL LETTRS LIKE THIS!!!), use (and often misuse) of fragments of {talk mode} abbreviations, a long {sig block} (sometimes even a {doubled sig}), and unbounded naivete. B1FF posts articles using his elder brother's VIC-20...(p. 60)
>
> [1993: Now It Can Be Told! My spies inform me that B1FF was originally created by Joe Talmadge..., also the author of the infamous and much-plagiarized "Flamer's Bible". The BIFF filter he wrote was later passed to Richard Sexton, who posted BIFFisms much more widely. Versions have since been posted for the amusement of the net at large. See also {Jeff K.} --ESR]
>
> :Jeff K.: The spiritual successor to {B1FF} and the archetype of {script kiddies}. Jeff K. is a sixteen-year-old suburbanite who fancies himself a "l33t haX0r", although his knowledge of computers seems to be limited to the procedure for getting Quake up and running. His Web page `http://www.somethingawful.com/jeffk' features a number of hopelessly naive articles, essays, and rants, all filled with the kind of misspellings, {studlycaps}, and number-for-letter substitutions endemic to the script kiddie and {warez d00dz} communities.

> Jeff's offerings, among other things, include hardware advice (such as "AMD VERSIS PENTIUM" and "HOW TO OVARCLOAK YOUR COMPUTAR"), his own Quake clan (Clan 40 OUNSCE), and his own comic strip (Wacky Fun Computar Comic Jokes).
>
> Like B1FF, Jeff K. is (fortunately) a hoax. Jeff K. was created by internet game journalist Richard "Lowtax" Kyanka, whose web site Something Awful (http://www.somethingawful.com) highlights unintentionally humorous news items and Web sites, as a parody of the kind of teenage {luser} who infests Quake servers, chat rooms, and other places where computer enthusiasts congregate. He is well-recognized in the PC game community and his influence has spread to hacker {fora} like Slashdot as well. (pp. 229-230)

Hacker argot in general is largely premised on creativity and humour. Language employing the use of wit, sarcasm, satire and quips is highly valued. For the uninitiated, such humour is often lost as these individuals are typically unfamiliar with the history behind folklorish witticisms and parodies like B1FF and Jeff K. Even dictionary excerpts from "The Jargon File", which provide specific definitions for terms, are likely to lose a significant amount of meaning on those unfamiliar with the hacker subculture and its history. As can be seen in the B1FF and Jeff K. citations, a general familiarity with cultural artefacts (both virtual and physical) such as software, web sites, and computers, and other role labels such as newbie and script kiddie, as well as the historical context of the jargon's development, all add further meaning to the passages. The linkages between all the various cultural elements affixed to a particular term or phrase come together to give each piece of jargon a more complete, and often multifaceted and many-layered definition.

As with other subcultures, role labels are used to situate individuals within the community. These labels are used to compartmentalize the various functions particular individuals serve or form of behaviour and attitude they become known for. In addition, each label often carries with it a value or a moral position and thus, serves to stigmatize in a negative or positive light. It should be noted that labels are interpreted differently depending on the particular group of hackers using them. To one group of hackers the term "cracker" might be looked upon with scorn, whereas another group might take pride in their title.

## DISCUSSION

This chapter highlighted a number of different elements of the hacker language, which separate and distinguish it from other cultures. The two broad areas of hacker argot that were discussed included techspeak and jargon.

Techspeak is not so much unique to the hacker subculture. Rather individuals working in fields related to technology frequently incorporate techspeak into their technical discussions. Given their keen interest in computers, and electronics more generally, Techspeak figures in quite centrally to hacker conversations. It provides them with a unique set of vocabulary that is specific to the types of artefacts and activities, which hackers commonly work with and make reference to.

While Techspeak may be seen as the more formal language of the hacker argot, hackers also have their own brand of informal jargon. As discussed in this

chapter, hacker jargon includes, but is not limited to, Netspeak, 31337SP34K (Elitespeak or Leet) and role labels.

Netspeak includes a number of uniquely identifiable styles of writing that have been developed to coincide with the particular online communication medium being used. For instance, while attempting to preserve the meaning and intent of the messages, a number of short forms and acronyms are used during real-time communication to help speed-up discussions. To compensate for the dialogue accessories normally present during people's face-to-face interactions, hackers also make use of intention conveying symbols and remarks, such as emoticons, to denote activity, emotionality, and intent while communicating online. In this way, a number of keyboard-based characters and combinations of other symbols come to hold special meaning to hackers. Non-hackers who make extensive use of the Internet to communicate with other individuals are also often "fluent" in Netspeak.

Leet is the exchange of letters for non-alphabetical characters, which the letters are seen to look or sound like. Some hackers see the use of Leet as a form of code, which is used so that non-hackers will be unable to understand what is being said. Certain individuals feel that Leet has a somewhat more noble history when compared to its current usage. The general argument is that Leet has become too simplistic, overused and no longer characteristic of "true" or "elite" hackers.

In general, hackers frown upon the excessive use of Netspeak and Leet. Making a number of spelling and grammatical errors (intentional or otherwise), overusing abbreviations, acronyms, and letter and number combinations makes writing both a nuisance to read and potentially incompressible. At the same time, an excess or inappropriate (i.e., non-satirical) use of Leet is seen as a blatant attempt to mimic the ways in which wannabe hackers feel "true" hackers communicate. As such, novice hackers have to not only learn what specific terms mean, they also have to follow the particular norms surrounding the use of jargon as they move between groups and communicate in different contexts.

The final form of jargon discussed in this chapter was role labels. As mentioned, these labels develop as ways to situate individuals within the culture and distinguish between different groups. Hacker jargon, of which role labels are just one example, is often based upon the folklore of the hacker subculture and therefore, holds special meaning only to those who are aware of the historical and interrelated cultural aspects[36] of the hacker community. By observing and beginning to understand the various linguistic elements of the subculture, one comes to find that hackers revel in creative wordplay, which is displayed by their often witty and sarcastic humour.

Adopting, understanding and employing hacker argot is important in the hacker community for at least a couple reasons. First, understanding what the different words and expressions mean allow individuals to contribute to

[36] For example, how the various labels associated with different hacker types are related to the activities and artefacts of the culture.

discussions and engage in the group's activities with a *shared level of comprehension*. Second, the ability to communicate fluently serves as a marker of insiderness (and thus, becomes an aspect of the hacker identity). Note the following passage from the "The Jargon File":

> As usual with slang, the special vocabulary of hackers helps hold their culture together -- it helps hackers recognize each other's places in the community and expresses shared values and experiences. Also as usual, _not_ knowing the slang (or using it inappropriately) defines one as an outsider, a mundane, or (worst of all in hackish vocabulary) possibly even a {suit}. All human cultures use slang in this threefold way -- as a tool of communication, and of inclusion, and of exclusion. (Raymond, 2000b, p. 2)

Understanding and using the language contribute to one's continuity within the community and are taken into account when determining the status of individuals. Individuals' use of certain forms of hacker jargon mark them as certain "types" and thus, also becomes used to identify what role designations they will be assigned. That is, use of particular words or styles of communication mark the individual as a newbie, script kiddy, "true" hacker, etc. Depending on the group the person is involved in, how he or she communicates with others will be seen differently. Within each group, shared understandings of what vocabulary is appropriate for their community will be negotiated and enforced informally through their discussions and activities.

Elements of the hacker argot exist both on and off the Internet. There are also certain terms and conventions of speech that are medium-specific, which have been adopted to reflect the various intricacies of a particular form of

communication (e.g., face-to-face interaction versus text-based communication). As was discussed in this chapter, a great deal of hacker-to-hacker communication over the Internet only conveys its intended meaning when it is seen in writing and not spoken. However, there are other elements of the hacker argot that only convey their intended (or extra) meaning when they are articulated verbally. As such, researchers examining the symbols of a particular subculture should be cognizant of and attend to such differences so as to provide a more complete understanding of not only how meaning is conveyed, but also the various ways in which meaning becomes relative to the medium, context, actors, and time period.

The hacker argot can also be seen as a reflection of their ideology. In particular, the hacker principles of creativity and anti-authoritarianism are quite evident in their vocabulary. As evidenced in this chapter, hackers, in developing their own unique style of speech, emphasize creative wordplay, develop their own language and grammar rules, and place value on satirical rhetoric that ridicules or condemns those who are seen as imposing conformity. Hackers are iconoclasts even in their use of language.

# CHAPTER SEVEN

# CONCLUSION

## SUMMARY

Until more recently it would have been difficult to characterize hackers as existing as a transnational subculture. While much of their activity still occurs in isolation, there has been a growing amount of information sharing occurring as wide area networks such as Bulletin Board Systems and the Internet have opened up the lines of communication and made it more feasible for the once geographically disparate group to form international networks. The current statement has attempted to describe the hacker community by working from the interactionist perspective and taking an ethnographic approach to examine the subculture's ideology and language, as well as how insiders define themselves and their activities.

By integrating insights acquired during the interviews and fieldwork, I was better positioned to represent the world of the hacker as hackers see it. The interview and field research data came together to provide a richer, more complete understanding of the experiential aspects of the hacker subculture than could have been achieved by using only one of these approaches. It is one thing to be told about how something happened or the way in which a particular object

functions and what it means, but it is quite another thing to be present as people are actually going about their activities and witness how reality is constructed and situationally defined through their everyday negotiations and interactions. Immersion within the actual life-worlds of hackers or, at the very least, certain aspects of their life-worlds such as online discussions and offline meetings, assisted in acquiring a better of sense of the types of things that interested hackers, the emotionality tied to their experiences, and the subtle qualities of these events that could only be gained from being there. By being able to follow these things up during later field excursions and interviews, I was provided with a greater sense of how hackers understand and actively work toward constructing their subculture. Over the course of the research I was able to demonstrate my genuine interest in wanting to learn about the subculture from those who were actively involved in its construction. In doing so, I was also able to develop the type of rapport necessary to be permitted to observe and participate in their interactions and activities and conduct upfront interviews with participants.

Previous research indicates that the term hacker has undergone a series of definitional shifts. Galvanized by claims-makers, including the media, government and computer security industry, within public discourse, "hacker" has moved away from its more positive non-deviant definition of computer programming genius to its present deviant meaning of computer criminal. A closer look at how hackers define themselves reveals that insider perspectives are often at odds with mainstream media portrayals of the community. Given that the

media tend to focus on the sensational in order to capture the public's attention, highlighting the criminal exploits of crackers (over the more mundane field of lawful hacking, as practiced by elite computer programmers) is very much in keeping with their agenda. However, this biased attention on the criminal realm of hackers stigmatizes other hackers who do not use their knowledge for malicious purposes.

Hackers criticize media portrayals of their community as it is felt that such representations are often inaccurate and depict the entire community as a homogenous group predominantly defined by certain individuals' illegal behaviour. In doing so, hackers see the media as perpetuating deviant stereotypes about all hackers to a public that is all too trusting about what is presented in the media.

Research for this thesis indicates that the hacker subculture is quite diverse. Individuals considering themselves hackers have a wide range of interests. In order to differentiate between the various actors within the hacker community insiders have developed a number of different role labels. These labels serve to distinguish individuals in terms of their level of knowledge and creative approach to problem-solving and the imputed ethics underlying the activities they engage in. For instance, these labels act as ways of differentiating the "good" true hackers or whitehats from the "bad" crackers or blackhats. Traditional hackers suggest that crackers and other malicious "hackers" such as

script kiddies, warez d00dz and cyberpunks are the ones that end up giving the subculture a bad name.

Although the subculture is quite diverse, characteristics such as the hacker ideology and language are shared more or less across the various local cultures of the hacker community. The hacker ideology or hacker spirit incorporates a number of principles that, as a whole, are unique to the subculture. However, hackers maintain that the hacker mindset is not so much unique to their community, but elements of their philosophy are employed by other "kindred spirits", including doctors and musicians.

Consistent with the overarching goal of *striving towards ever-greater understandings of how things work*, the principles of the hacker spirit include:

1. Higher understanding requires an unorthodox approach – be inventive, think outside the box;
2. Understanding things, solving problems and generating new ideas requires hard work – dedicate yourself to this task;
3. Learning should be self-directed – learn by doing;
4. A hacker's learning time is precious – share your knowledge with others;
5. You are evaluated on what you know and how you learn – looks and degrees are not important – show us your skill;
6. People in positions of power often value and impose conformity – this attitude must be rejected as it stifles creativity – mistrust authority; and,
7. Hackers require as much information as possible to understand things – access to information should be free and unrestricted.

The ideology of today's hacker is closely related to the "Hacker Ethic" coined by Levy (1984), which he used to describe the ideology of the first generation of hackers. However, unlike the first generation, subsequent generations of hackers have employed the hacker ideology to rationalize an increasing range of activities

that are often illegal. As a result, traditional hackers chastise the younger generation of hackers for not properly adopting and utilizing the hacker mindset and only engaging in the sorts of superficial things necessary to make people think that they are hackers.

This thesis has also argued that there is a hacker argot, primarily composed of two distinctive forms of vocabulary: techspeak and jargon. Techspeak is the formal technical language of the hacker subculture and is shared with others working in the area of computers and electronics. Aspects of techspeak have been formalized in dictionaries and the professional manuals of the computer profession. Techspeak is used as a way of more precisely communicating about the different objects and activities that are specific to the hacker culture (e.g., operating systems, disks, networks, booting, formatting).

Jargon on the other hand is the slang of the hacker subculture. Three aspects of hacker jargon discussed in this thesis were Netspeak, 31337SP34K (Elitespeak or Leet) and role labels. Netspeak includes the different symbols (e.g., emoticons such as the sideways smiley face), short forms (e.g., cya = see you) and acronyms (e.g., lol = laugh out loud, np = no problem) used by hackers and others who make extensive use of the Internet to speed-up online communication and convey intention and emotionality.

Leet is the exchange of non-alphabetical characters and combinations of these symbols for the letters that these characters look or sound like (e.g., 1337 = Leet, m8 = mate). For some, Leet is seen as a sort of code that outsiders cannot

understand and online censoring programs do not recognize. Some hackers argue that Leet had a more noble history, but given the way in which it is currently used, typically by script kiddies, warez d00dz, and newbies, it has become laughable and is used by *real* hackers to identify these "lame" individuals.

Role labels such as cracker, newbie, troll and leecher have been developed by hackers to situate the different subcategories of hackers within the community and distinguish between the different groups. Hacker jargon such as role labels is often based on the folklore of the community. As such, the meaning associated with each of the different terms can only be understood by acquiring an understanding of the subculture's history, inside jokes and stories.

## THEORETICAL AND SUBSTANTIVE CONTRIBUTIONS

Beyond the findings already discussed in the last section, there are at least twelve theoretical and substantive conclusions that can be drawn about the hacker subculture. First, findings confirm the existence of a hacker subculture. Although hackers' subcultural interests are diverse and the subculture is quite complex, the consistency of identifiable and unique characteristics such as the community's ideology and argot support this conclusion. The subculture is developed through individuals' interactions within a series of local subgroups and overlapping activities that are mediated through the Internet, subcultural publications, outsider representations, and local, national and international gatherings. Through these communication channels individuals directly and indirectly interact with one another and negotiate a mutual set of perspectives and

subsequently attribute meanings to themselves and the world they see. In this way, elements of local subcultures, developed within more geographically restricted settings and channels of interaction, are shared across groups, and contribute to the formation of a transnational subculture.

Second, hackers tend to place a significant amount of blame on the media and a subsequently uniformed public for perpetuating misunderstandings and misleading definitions about the hacker community. However, given the highly debated nature of the term within the hacker culture itself - as individuals whom consider themselves to be hackers defend different meanings of the term to suit their particular interests and perspectives - they further confuse any concrete or enduring definition. Therefore, definitions are constantly being redefined as individuals negotiate and defend the term from others both inside and outside the community. Consequently, the meaning of "hacker" is necessarily relative as definitions change over time and within different contexts, and differ from group to group, and individual to individual.

Third, this study has reinforced a key point of labelling theory (Becker, 1963) regarding the implications of being labelled. That is, although a person labelled as a hacker may have never committed a rule-breaking act such as engaging in the unauthorized access of a computer system, by virtue of the hacker label, his or her public identity has been diminished. By being associated with a label that publicly identifies a group of people as rule-breakers (i.e., computer criminals), each individual hacker is consequently identified by outsiders in terms

of traits associated with the label – e.g., socially inept, young, criminal, geek. This in turn has consequences for how the hacker is perceived and feels he or she is perceived by outsiders.

Fourth, to deal with their deviant public identity, hackers engage in stigma management techniques. Similar to the *condemnation of the condemners* technique of neutralization identified by Sykes and Matza (1957)[37], hackers blast the media for categorizing all hackers as computer criminals. Consequently, hackers indicate that the media are at fault for perpetuating the deviant image of hackers and making celebrities out of inappropriate criminal role models, which wannabe hackers end up replicating. Thus, the media are seen as also having a hand in perpetuating computer crime. As another way of managing stigma, hackers apply various labels to the different actors within the hacker subculture to distinguish the "good" from the "bad." These labels are used in a claims-making bid to "properly" define the malicious crackers from the non-malicious hackers. Furthermore, hackers link their ideology to the mindset of individuals whom society looks upon favourably such as doctors and athletes. In doing so, hackers attempt to promote a more positive image of their subculture.

Fifth, while most hackers disagree with being labelled as criminals, they very much agree with the counterculture overtones of their ideology and activities. Recognizing that outsiders see their subculture as deviant, hackers feel

[37] Along with this technique it would appear that hackers also employ other techniques of neutralization identified by Sykes and Matza (1957) such as *denial of injury*, *denial of victim*, and *appealing to higher loyalties*. This assertion, however, was not directly examined in thesis and therefore, would constitute an area for future investigation.

that their ideology and activities are normal and often admirable. Like the jazz musicians described by Becker (1963) or the mystics in Simmons' (1973) study, hackers see their perspective as being elite and a better way of doing things and seeing the world than other outsider belief systems. Freedom of information over ownership of information, creativity over conventionality, hard work and self-direction over indolence, intellectualism over looks and style, unorthodoxy over conformity, these are all highly valued and very noble pursuits within the hacker subculture.

Sixth, by formulating an ideology built on principles that are not only consistent with and compliment one another, but also resonate with outsider beliefs such individualism, creativity, hard work, and freedom, aspects of the hacker ideology may also be valued by outsiders. However, since outsiders see hackers and their associated characteristics as deviant, it is unlikely that they would admit to the validity of such a belief system.

Seventh, by invoking principles of the hacker spirit to rationalize their actions, hackers present their activities as justified and normal behaviour. In this way, the explication of their ideology within specific situations acts as a vocabulary of motive, a way of normalizing their behaviour and thus, a further stigma management technique.

Eighth, by interacting with others who share a common set of perspectives, where people's beliefs and attitudes are supported, the ideology of the group is reinforced and normalized. During their interactions hackers are able

to espouse their ideals within a relatively non-hostile environment and therefore, are not reprimanded for their views. If an individual does not find support for his or her beliefs within one group, given the diversity of the subculture, other subgroups of hackers may engage in the types of activities the person is interested in and relate to the same ideology as the individual.

Ninth, as new individuals enter into the hacker community and introduce new interpretations, as outsiders make claims against the subculture, and as long-standing insiders leave the community, hackers are constantly negotiating their reality and the subculture necessarily evolves. Therefore, the subcultural characteristics of the hacker community are relative across time. As evidenced by the varied uses of the term hacker and the meanings placed on aspects of the hacker ideology and language, insider and outsider interpretations are also relative and intersubjectively defined through their interactions with others.

Tenth, beyond serving as a way of communicating more specific understandings about subcultural objects and activities, employing the hacker argot also acts as a mark of insiderness and is used to identify the type of hacker a person is (e.g., script kiddy, lamer, old-school hacker). What is and is not appropriate use of the hacker language and what actually constitutes the vocabulary of the language is defined and enforced differently in the various subcommunities. In addition, the meaning underlying a particular word is also relative to the communication medium being used. For instance, certain words

take on different meanings when they are viewed (e.g., Micro$oft) compared to when they are heard (e.g., Microsoft).

Eleventh, the hacker argot can also be seen as a reflection of the hacker ideology. The creative use of language, invention of new words and grammatical rules, and development of vocabulary and idioms focused on deriding institutions and corporations that are seen as imposing conformity, demonstrate hackers' creative and anti-authoritarian mindset. The way in which their ideology is intertwined within the other characteristics of the subculture such as their activities and artefacts is quite evident. Further research would permit for a more developed analysis of this insight.

Finally, while online research is essential in understanding the hacker community, there are some limitations to this form of investigation that must be taken into consideration and minimised wherever possible. A significant amount of research for this thesis was based on my online interactions with hackers. Perhaps the main reason for engaging hackers in this way is that the Internet represents a significant communication medium for this group. As such, it is necessary to be involved in and witness hackers' interactions as they take place online. I would argue that this component of the research, with a group that makes extensive use of the Internet, is just as important as it is to meet with them face-to-face and be a part of and observe the types of activities they engage in off the Internet. Although it has become increasingly possible to physically meet with these individuals (at least in my area) and develop further offline contacts,

the Internet helps to facilitate interviews and interactions with other hackers in different parts of the world.

The Internet is one of the most significant artefacts of the hacker culture. Hackers built the Internet and through it they communicate their cultural understandings, create their identities and give meaning to symbolic objects, develop their argot, formulate norms and perspectives, and engage in online activities. As such a central component of their culture, the Internet must necessarily be a key medium through which the ethnographer investigates this subculture.

Although it is indeed necessary to engage this culture through online fieldwork, it is equally essential that the researcher interacts with this community on a face-to-face basis and be cognisant of the limitations of both on- and off-line investigation. The key limitation of online research, which in some cases actually benefits the researcher, is mediated distance. A central feature of mediated distance that limits online interactions in some instances, while facilitating them in others, is one's perceived anonymity. As a result of these two aspects of online communication, the researcher has to try to overcome obstacles that are not present, or are present in different ways, when interacting on a face-to-face basis.

The ultimate limitation posed by the anonymity that typically results from mediated distance is not knowing for sure who you are communicating with. Someone can choose to pose as another person online, which can significantly, if not totally, undermine the research effort. There are certain cues that we can look

for that can help us to identify other people online. The researcher can take a number of different measures to encourage truthfulness and verify the authenticity of a respondent's identity and remarks, but at some point it ultimately comes down to trust. The researcher has to not only trust that the other parties are who they say they are, but also that they are not trying to deceive us in other ways during the course of our investigation. In order to establish this sort of trust it is essential to engage in rapport building both on and off the Internet. When possible, a good approach to dispel informants' suspicions is to have other parties vouch for the authenticity of your research.

With a limited range of online dialogue accessories, it can become difficult to assess the truthfulness of people's responses. However, the other side of anonymity is that participants are likely to be more forthcoming about their experiences and perspectives if they trust that you are who you say you are and are interested in providing you with their viewpoints. For this reason, developing rapport, assuring confidentiality, and verifying the purposes of your research and your affiliation are paramount. By being open and honest with participants, the hope is that they will do the same for you.

The limited range of dialogue accessories also inhibits our understandings when communicating in real-time over the Internet. However, if the researcher does not understand something, he or she can easily ask for clarification. This can usually be done during the interview and sometimes even months after the

interview takes place. In all fairness to respondents, if necessary, it is best to follow-up with them as soon as possible.

Another result of mediated distance is that the researcher only knows what is happening on the other end of the communication by having the responding party make this known. Someone who is multi-tasking might not be completely focused on the interview. Maybe the individual is simultaneously involved in a series of different online communications or is doing something else away from the computer. Technical difficulties such as power outages, software failures, and Internet slowdowns also impede on the ability of the researcher to conduct online research.

Mediated distance also allows people to justify a lack of response based on factors out of their control, without you easily being able verify the veracity of their claims. "My computer crashed." "The power went out." "I had to answer the door or telephone." Whether honest or not, like face-to-face interviews, what matters is that the researcher attempt to minimize controllable distractions and encourage honesty. After all, both the researcher and the participants have a vested interest in the results of the study. Some recommendations to help reduce distractions and encourage straightforward responses include:

- Schedule interviews for when respondents can give you their complete attention;
- Recognize that long interviews will likely require breaks for both parties and may have to be carried out over the course of a few sessions;
- Let respondents know how long the interview could last for;
- Be attentive and interested in what respondents are saying, because if you are not interested it is likely that they will not be either;

- Make questions meaningful and understandable;
- Emphasize that you are interested in *their* experiences as they truly are the star of the show;
- Try to make participants feel as comfortable as possible about their responses and if they do not want to answer a question, make sure they know that skipping questions is not a problem;
- If there are any special words or conventions that you want to use to help make the interview go smoother, make these clear at the outset of the interview; and,
- Develop as much rapport as possible with informants before interviewing them.

## DIRECTIONS FOR FUTURE RESEARCH

At the outset of this research I had planned to investigate and report on the following six characteristics of the hacker subculture: (a) ideology; (b) argot; (c) activities; (d) artefacts; (e) norms; and, (f) identity. The initial process of involvement into the hacker "career" constituted an additional area of inquiry that I had hoped to analyse. However, given the focus devoted to examining the hacker ideology and argot, as well as definitional issues surrounding the term hacker, I was unable to report on the data I had gathered on the other five areas. As demonstrated by the outline in Appendix A, a significant amount of material was collected on these topics and has been preliminarily coded. Analysing and integrating findings on each of these areas can only lead to a more complete understanding of the hacker subculture.

As Huss (1998) also advocates, it is necessary to collect data on the full range of hacker activities as described and enacted by participants, and not just their (outsider defined) criminal behaviours. Therefore, data should be collected on the different groups of hackers from script kiddies to elite traditional hackers.

This type of inductive exploratory research will allow social scientists to identify more specific areas for future empirical studies.

Findings from this thesis indicate that subcultural characteristics such as the formation of perspectives and creation of linguistic variants are not unique to the hacker community. For instance, other groups such as mountain climbers and professional thieves develop their own argot to account for the different activities they engage in and new meanings given to objects in their community. Although not a specific focus of this thesis, it is recommended that researchers continue to identify, investigate and verify the legitimacy of the generic social processes that occur transcontextually and thus, underlie the social construction of reality (Prus, 1996, 1997).

The hacker subculture is diverse and quite complex. Without exploring how hackers actually accomplish their activities by engaging them about their perspectives and examining their behaviour, any outsider definition of the community is bound to be limited. Although this thesis is preliminary in certain ways, it has paved the road for a more informed understanding of the hacker subculture as it is socially constructed during the course of hackers' everyday interactions.

# BIBLIOGRAPHY

Arbaugh, J. (1999). Cyberdeviance. In C. H. McCaghy, T. A. Capron, & J. D. Jamieson (Eds.), Deviant behavior: Crime, conflict, and interest groups (Fifth ed.). (pp. 366-386). Toronto, ON: Allyn and Bacon.

Arnold, D. O. (1970). A process model of subcultures. In D. O. Arnold (Ed.), The sociology of subcultures. (pp. 112-118). Berkeley, CA: The Glendessary Press.

Bailey, C. A. (1996) A guide to field research. Thousand Oaks, CA: Pine Forge Press.

Becker, H. (1963). Outsiders. New York, NY: Free Press.

Becker, H. (1970). Sociological work: Method and substance. Chicago: Aldine.

Becker, H. & Geer, B. (1970). Participant observation and interviewing: A comparison. In W. Filstead (Ed.), Qualitative methodology (pp. 133-142). Chicago: Rand McNally.

Becker, H., Geer, B., Hughes, E. C., & Strauss, A. L. (1961). Boys in white: Student culture in medical school. Chicago: University of Chicago Press.

Berg, B. L. (2001). Qualitative research methods for the social sciences. (Fourth ed.). Toronto, ON: Allyn and Bacon.

Blumer, H. (1969). Symbolic interactionism. Berkeley, CA: University of California Press.

Burgess, R. G. (1991). Sponsors, gatekeepers, members, and friends: Access in educational settings. In W. B. Shaffir & R. B. Stebbins (Eds.), Experiencing fieldwork: An inside view of qualitative research. (pp. 43-52). Newbury Park, CA: Sage Publications, Inc.

California State University (2003). Hanging with hackers puts computer crime in focus. Public Affairs Office Web Site. [On-line]. Available: www.csus.edu/news/050401loper.html.

Chandler, A. (1996). The changing definition and image of hackers in popular discourse. International Journal of the Sociology of Law, 24, 229-251.

Chawla, R. (2001, May 17). Hackers beware! State Hornet Online. [Online]. Available: http://webpages.csus.edu/~doc/HackersBeware_StateHornet5-17-01.pdf

Churchill, D. (2000, September 13). Casting a net of security. The Hamilton Spectator. [On-line]. Available: http://www.hamiltonspectator.com/the_internet/212375.html

Clarke, M. (1974). On the concept of sub-culture. British Journal of Sociology, 25, 428-441.

Clough, B. & Mungo, P. (1992). Approaching zero: Date crime and the computer underground. London: Faber & Faber.

Cohen, A. K. (1955). Delinquent boys. Glencoe, IL: Free Press.

Cooley, C. H. (1922). Human nature and the social order. New York: Charles Scribner's Sons.

Copes, H. & Huss, S. (1999). Claims and counter-claims in cyberspace: The social construction of computer crime. Paper presented at the meeting of the Society for the Study of Social Problems, Chicago, IL.

Defcon. (June 2001). Defcon 9 web site. [On-line]. Available: http://www.defcon.org.

Duff, L. & Gardiner, S. (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.

Ferguson, I. (1999). Sacred realms and icons of the damned: The ethnography of an internet-based child pornography ring. Masters thesis prepared for the Department of Sociology and Anthropology Carleton University, Ottawa, Ontario, Canada.

Fetterman, D. M. (1991). A walk through the wilderness: Learning to find your way. In W. B. Shaffir & R. B. Stebbins (Eds.), Experiencing fieldwork: An inside view of qualitative research. (pp. 87-96). Newbury Park, CA: Sage Publications, Inc.

Fine, G. A. (1983). Shared fantasy: Role-playing games as social worlds. Chicago, IL: University of Chicago Press.

Fine, G. A. (1987). With the boys: Little league baseball and preadolescent culture. Chicago, IL: University of Chicago Press.

Fine, G. A. & Kleinman, S. (1979). Rethinking subculture: An interactionist analysis. American Journal of Sociology, 85(1), 1-20.

Glaser, D. (1956), Criminality theories and behavioral images. American Journal of Sociology, 61, 433-444.

Goode, W. J. (1957) Community within a community: The professions. American Sociological Review, 22(2), 194-200.

Gordon, M. M. (1970). The subsociety and the subculture. In D. O. Arnold (Ed.), The sociology of subcultures. (pp. 150-163). Berkeley, CA: The Glendessary Press.

Hafner, K. & Markoff, J. (1991). Cyberpunk: Outlaws and hackers on the computer frontier. London: Fourth Estate.

Hollinger, R. C. (1988). Computer hackers follow a Guttman-like progression. Sociology and Social Research, 72(3), 199-200.

Humphreys, L. (1975). The tearoom trade: Impersonal sex in public places. Chicago, IL: Aldine Publishing Company.

Huss, S. T. (1998). Hackers: Practices, Motivations, and Identity. Master's Thesis, University of Tennessee, Knoxville.

Ibarra, P. R. & Kitsuse, J. I. (1993). Vernacular constituents of moral discourse: An interactionist proposal for the study of social problems. In G. Miller & J. A. Holstein (Eds.), Constructionist controversies: Issues in social problems and theory. (pp. 21-54). Hawthorne, NY: Aldine de Gruyter.

Isocrates. (1928). Isocrates: To Demonicus, to Nicocles, to Nicocles or the Cyprians, Panegyricus, To... (G. Norlin, Trans.). Cambridge, MA: Harvard University Press.

Irwin, J. (1970a). Deviant behavior as a subcultural phenomenon. In D. O. Arnold (Ed.), The sociology of subcultures. (pp. 109-111). Berkeley, CA: The Glendessary Press.

Irwin, J. (1970b). Notes on the present status of the concept of subculture. In D. O. Arnold (Ed.), The sociology of subcultures. (pp. 164-170). Berkeley, CA: The Glendessary Press.

Jordan, T. and Taylor, P. (1998). "A sociology of hackers". The Sociological Review, 46(4), 756-780.

Kleinknecht, S. (2000). Life is what *we* make it: An ethnographic endeavour into the virtually enacted life-world of Kinship, an online role-playing community. Unpublished undergraduate thesis. University of Waterloo, Waterloo, Ontario, Canada.

Letkemann, P. (1973). Crime as work. Englewood Cliffs, NJ: Prentice-Hall, Inc.

Levy, S. (1984). Hackers: Heroes of the computer revolution. New York: Bantam Doubleday Dell.

Liebow, E. (1967). Tally's corner: A study of Negro streetcorner men. Boston, MA: Little, Brown and Company.

Liebow, E. (1994). Tell them who I am: The lives of homeless women. New York: The Free Press.

Loseke, D. R. (1999). Thinking about social problems: An introduction to constructionist perspectives. Hawthorne, NY: Aldine de Gruyter, Inc.

McCaghy, C. H. & Capron, T. H. (Eds.). (1997). Deviant behavior: Crime, conflict, and interest groups (Fourth ed.). Boston, MA: Allyn and Bacon.

Mead, G. (1934). Mind, self and society. (edited by Charles W. Morris). Chicago: University of Chicago Press.

Miller, W. B. (1958). Lower class culture as a generating milieu of gang delinquency. Journal of Social Issues 14, 5-19.

Mills, C. W. (1940). Situated actions and vocabularies of motive." American Sociological Review, 5, 904-913.

Mitchell, R. G., Jr. (1983). Mountain experience. Chicago, IL: University of Chicago Press.

Platt, C. (1997). Anarchy online: Net sex / net crime. New York : Harper Prism.

Prus, R. (1996). Symbolic interaction and ethnographic research: Intersubjectivity and the study of human lived experience. Albany, New York: State University of New York Press.

Prus, R. (1997). Subcultural mosaics and intersubjective realities: An ethnographic research agenda for pragmatizing the social sciences. Albany, New York: State University of New York Press.

Prus, R. (1999). Entertainment in the making: Intersubjective contexts and participatory roles. Unpublished manuscript, University of Waterloo, Waterloo, Ontario.

Prus, R. & Irini, S. (1980). Hookers, rounders, & desk clerks: The social organization of the hotel community. Toronto, ON: Gage. (Reissued, 1988, Salem, WI: Sheffield Publishing Company).

Raymond, E. S. (2000a). How to become a hacker. [On-line]. Available: http://www.tuxedo.org/~esr/faqs/hacker-howto.html

Raymond, E. S. (ed.). (2000b). The on-line hacker jargon file, version 4.2.2. [On-line]. Available: http://www.tuxedo.org/~esr/jargon/

Rheingold, H. (1991). Virtual reality. London: Mandarin.

Rheingold, H. (1993) The virtual community: homesteading on the electronic frontier. New York: Harper Perennial.

Rosoff, S., Pontell, H & Tillman, R. (1998). Computer crime: Hackers, Phreaks, and Cyberpunks. In H. N. Pontell (Ed.), Social deviance: Readings in theory and research (Third ed.). (pp. 397-411). Englewood Cliffs, NJ: Prentice Hall.

Roth, J. A. (1970). Comments on "secret observation". In W. J. Filstead (Ed.) Qualitative methodology: Firsthand involvement with the social world. (pp. 278-280). Chicago, IL: Markham Publishing Company.

Shaffir, W.B. & Stebbins, R. (Eds.). (1991). Experiencing fieldwork: An inside view of qualitative research. Newbury Park, CA: Sage Publications, Inc.

Shibutani, T. (1955). Reference groups as perspectives. American Journal of Sociology, 60, 562-569.

Simmons, J. L. (1973). Maintaining deviant beliefs. In E. Rubington & M. S. Weinberg (Eds.), Deviance: The interactionist perspective. (pp. 308-314). New York: The Macmillon Company.

Spector, M. & J. I. Kitsuse. (1987). Constructing social problems. Hawthorne, NY: Aldine de Gruyter.

StankDawg. (2002). A history of "31337SP34K." 2600: The Hacker Quarterly, 19(3), 40-41.

Sterling, B. (1992). The hacker crackdown: law and disorder on the electronic frontier. New York: Bantam Books.

Strauss, A. (1982). Social worlds and legitimation processes. In N. K. Denzin (Ed.) Studies in symbolic interaction 4. (pp. 171-190). Greewich, CT: JAI.

Strauss, A. (1984). Social worlds and their sementation processes. In N. K. Denzin (Ed.) Studies in symbolic interaction 5. (pp. 123-139). Greewich, CT: JAI.

Strauss, A. (1993). Continual permutations of action. Hawthorne, NY: Aldine de Gruyter.

Sutherland, D. (1947). Principles of criminology (Fourth ed.). Philadelphia: J. B. Lippincott.

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

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

Taylor, P. A. (2001). The social construction of hackers as deviants. In A. Thio and T. C. Calhoun (Eds.), Readings in deviant behavior (Second ed.). (pp. 283-292). Toronto, ON: Allyn and Bacon.

Taylor, S. J. & Bogdan, R. (1984). Introduction to qualitative methods: The search for meanings. New York: Wiley.

The Mentor. (1986). The conscience of a hacker. Phrack, 1,7 File 3. [Online]. Available: http://www.phrack.org/show.php?p=7&a=3.

Turkle, S. (1997). Life on the screen. New York: Simon and Schuster.

Wax, R. (1971). Doing fieldwork: Warnings and advice. Chicago: University of Chicago Press.

Whyte, W. F. (1943). Street corner society: The social structure of an Italian slum (Thirteenth Impression, 1970). Chicago, IL: University of Chicago Press.

# APPENDIX A: CODING SHEET

DEFINITION (1)

11 Choice Quote

12 Miscellaneous Definition

13 Classifying & Hierarchy

14 General Application

15 Hacker/Cracker

16 Hats

17 Media

INVOLVEMENT (2)

21 Choice Quote

22 Miscellaneous Involvement

23 Closure

24 Made Inv. easier

25 Group / Subcultural

26 Multiple Routes

27 Obstacles

28 Recruitment

29 Reservations

2a Seekership

2c Learning the Ropes

IDEOLOGY (3)

31 Choice Quote

32 Miscellaneous Ideology

33 Anti-authoritarianism

34 Creativity

35 Elitism

36 Freedom of Speech & Information

37 Historical Knowledge

38 Knowledge

39 Learning

3a Push Limits of Tech

3b Rationalizations & Justifications

3c Sharing Information

ACTIVITY (4)

41 Choice Quote

42 Miscellaneous Activity

43 Coding & Ingenuity

44 Conference

45 Feelings

46 Group vs. Alone

47 Hardware: Building & Mods

48 Humour

49 Malicious

4a Meetings

4b Referencing Materials

4c Social Behaviour

4d Techtalk

4e Time Spent

LANGUAGE / ARGOT (5)

51 Choice Quote

52 Miscellaneous Language

53 Conventions

54 Jargon

55 Leet Speak

56 Program Language

57 Techspeak

RULES & NORMS (6)

61 Choice Quote

62 Miscellaneous Rules

63 Enforcement

64 Gender

65 Opensource

66 Learning the Ropes

67 Security

68 Up-to-date re: tech

IDENTITY (7)

71 Choice Quote

72 Miscellaneous Identity

73 Background

74 Deviance

75 Difference

76 Handle

77 Icons

78 Mindset

79 Online vs. Offline

7a Presentation of Self

7b Reputation

7c Roles

7d Stereotyping

ARTEFACTS (8)

81 Choice Quote

82 Miscellaneous Artefacts

83 Food & Beverages

84 Literature (books & mags)

85 Personalized Items

86 Technology & Gadgets

87 Virtual Artefacts

LIMITATIONS (9)

91 Choice Quote

92 Miscellaneous Limitations

93 Gatekeepers

94 Non-face-to-face

95 Technological

96 Trust & Rapport

MISCELLANEOUS (11)

aa Choice Quote

bb Miscellaneous Misc.

cc History of Hacking

dd Motive

ee One-upsmanship

ff Subculture

gg Legality & ethics

hh Sources of info.

# APPENDIX B: "THE CONSCIENCE OF A HACKER"

(Article from Phrack magazine)

```
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
The following was written shortly after my arrest...

                    \/\The Conscience of a Hacker/\/

                                    by

                            +++The Mentor+++

                    Written on January 8, 1986
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
        Another one got caught today, it's all over the papers.
"Teenager Arrested in Computer Crime Scandal", "Hacker Arrested
after Bank Tampering"...
        Damn kids.  They're all alike.

        But did you, in your three-piece psychology and 1950's
technobrain, ever take a look behind the eyes of the hacker?  Did
you ever wonder what made him tick, what forces shaped him, what
may have molded him?
        I am a hacker, enter my world...

        Mine is a world that begins with school... I'm smarter
than most of the other kids, this crap they teach us bores me...
        Damn underachiever.  They're all alike.

        I'm in junior high or high school.  I've listened to
teachers explain for the fifteenth time how to reduce a fraction.
I understand it.  "No, Ms. Smith, I didn't show my work.  I did
it in my head..."
        Damn kid.  Probably copied it.  They're all alike.

        I made a discovery today.  I found a computer.  Wait a
second, this is cool.  It does what I want it to.  If it makes a
mistake, it's because I screwed it up.  Not because it doesn't
like me...
                Or feels threatened by me...
                Or thinks I'm a smart ass...
                Or doesn't like teaching and shouldn't be here...
        Damn kid.  All he does is play games.  They're all alike.
```

And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.

"This is it... this is where I belong..."

I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...

Damn kid. Tying up the phone line again. They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals.

You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

+++The Mentor+++