Université de Montréal

The Integration of the Computer Hacker in the Information Economy

par

Christopher K. Assié

Département de sociologie,

Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de
Maître ès sciences (M.Sc.)

Août, 2001

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé:

The Integration of the Computer Hacker in the Information Economy

présenté par

Christopher K. Assié

a été évalué par un jury composé des personnes suivantes:

Deena WHITE	président du jury
Mona-Josée GAGNON	directeur de recherche
Arnaud SALES	membre du jury

Mémoire accepté le: 10 décembre 2001

Résumé

Cette étude s'intéresse au rapport entre le hacker d'ordinateur et l'économie de l'information. L'étude utilise la définition du hacker comme un enthousiaste de l'informatique qui adhère à l'éthique du hacker et qui possède la compétence technique permettant de circonvenir les obstacles technologiques et d'ainsi créer des produits technologiques innovateurs. L'observation participante d'une conférence de hackers et l'analyse du contenu de courriers électroniques sont utilisés pour ajouter à la revue de littérature. Sont particulièrement discutés les points suivants. D'une part il est question du type de rapport au pouvoir que les hackers entretiennent au sein de l'économie de l'information. D'autre part la question de la relation précaire entre les hackers et les médias fait l'objet d'un développement. Enfin les débats à l'œuvre au sein des groups de hackers relatifs au caractère politique de leur actions sont examines. La théorie d'adaptation sociale de Merton est appliqué à la situation conflictuelle entre les buts culturelles d'aptitude technologique et les méthodes acceptable de démontrer l'innovation, la créativité et la manière d'acquérir les connaissances. Tous ces éléments aident à illustrer comment les hackers peuvent être vus comme un groupe contestataire déterminé à légitimer leurs sources de connaissances et à changer les relations sociales entre les consommateurs et les producteurs des technologies programmables.

Mots clés: ordinateur, crime, politique, économie, hacktivism, déviance.

Abstract

This study questions the relationship between the computer hacker and the information economy. By building on previous works, a definitional framework is established to define the hacker as ac computer enthusiast who has adopted the spirit of the hacker ethic and has the technical ability to circumvent barriers in order to create innovative technological artefacts. Participant observation of a hacker conference and a content analysis of a hacker list server are used to enhance the literature review. A discussion of how hackers represent new powerbrokers in the information society and how their influence is exerted leads to an examination of the precarious relationship that hackers have with mainstream media. The conflicting view within the computer underground regarding the political use of hacking is also examined. Merton's theory of social adaptation is applied to the conflict between the cultural goals of technological proficiency and the acceptable methods of demonstrating innovation, creativity and of acquiring knowledge. These elements help to illustrate how hackers can be interpreted as a rebellious group determined to legitimize their knowledge base and to challenge the social relationship between users and producers of programmable technologies.

Key Words: computer, crime, politics, economics, hacktivism, deviance.

Table of Contents

List of Figures

Remerciement/Acknowledgement

Je remercie sincèrement Mona-Josée Gagnon pour toute son aide.

I would like to thank Rebecca Purdy, Robin Fitzgerald and Dorothy Hepworth for their help as well.

Chapter 1 – Introduction

The beginning of the twenty-first century is marked by the intensification of a process that was well underway in the later half of the twentieth century, namely, the development of the information society. A two-fold process has occurred; the first being the rapid development of new information technologies while the second is the international division of labour (Castells 1996: 106). Technologically advanced industrial countries, the first world of yesteryear, have allowed low-skilled manufacturing to move to low-wage newly industrialized countries as part of a plan to specialize in the production of services and knowledge products. Industrial output has been consistently declining in Western Europe and North America while Asia and Latin America have seen dramatic increases in industrial investment in the last decade (Castells 1996: 107-145). The gap created by de-industrialization of production in the first world is being filled by 'knowledge' workers producing the new informational technologies, which supposedly will herald humanity into another phase of social and economic development (Toffler 1971: 187).

There is no greater symbol of the information economy than the Internet. The Internet is a system of interconnected computers that transfer data at phenomenal speeds through a vast array of telephone networks, allowing individuals to communicate and conduct business with each other throughout the world. An American

invention, its original purpose was to allow researchers at various universities the remote use of powerful expensive computers by login from their less costly computers in research centres throughout the United States. For many people, the world changed in 1994 when rapid hypertext and picture files could be transferred through what was called the World Wide Web. The Internet was intended to change the very fabric of human interaction and experience as the world would eventually be 'connected'. Thus, students in Canada could interact online with students in Zimbabwe, political dissidents in China could speak to activists in France, and the world would increasingly become a smaller place. The Internet was dubbed the 'Information Superhighway' and newspapers and magazines suddenly produced an 'Internet section'. A mere five years after its explosive debut, the Information Superhighway has disappeared. In its place, the Internet is fulfilling a more important goal and doing more than just binding communication gaps between individuals. It is now helping bridge the gap between business and consumers through E-business or E-commerce[1].

As of July 1997 more than 74 million Internet users existed, of which 56.8 percent of users lived in North America, while another

[1] In 1995 4,562 stories from media outlets throughout the world framed the Internet as the "information superhighway" while only 915 articles discussed it as e-commerce. By 1999 the number of articles with the information highway imagery went down to 842 while an astronomical 20,641 articles framed the Internet as a tool for commerce (Solomon 2000: 11-13).

20.3 percent lived in Europe and 17.6 percent in Asia (the majority of which were located in Japan and Hong Kong) (Pearson 1998: 59). Users double each year and it was forecasted that there would be over 600 million cyber-citizens online by the year 2001. This latest technological development has brought with it a growing awareness of a new group of people named hackers. This category of cyber-citizen differs from the rest of the Internet community because of their facility with technology as well as their particular philosophical beliefs. Philosophically, hackers tend to feel contempt for the constraints on free speech and disgust for barriers, as they spend an inordinate amount of time circumventing technological impediments and spreading the gospel of hacking. Whether the barriers exist due to poor technological construct or due to restrictive corporate licensing schemes, hackers build and share solutions to what they interpret as illegitimate limitations.

This new category of computer enthusiast is composed of a fascinating collection of individuals who range in age, nationality and gender. However, they are united by core beliefs, even though many may have trouble articulating their philosophies. To a hacker, technology is pleasurable and through technology great things can be created both collectively and by the individual. While hackers compose marginal elements of the technological society, they are simultaneously central to its development. By pushing the boundaries

of computer programming they illustrate and define the potential that these new tools posses.

The media hysteria that surrounds hackers is a fascinating phenomenon in and of itself. While hackers are publicly denounced as either vandals or terrorists, public sentiment is far from uniform on the subject (Taylor 1999: 174). When it comes to computer trespassing, the public is often quite sympathetic to perpetrator. A sentiment of satisfaction seems to exist in seeing a young individual outsmart a large faceless corporate entity by hacking into their web site. As long as damage is kept to a minimum and the issue stays within the realm of digital ones and zeroes, many have a hard time identifying with the 'loss' a company faces.

Hackers present a paradox; while they are marginal elements of society they are also perfect examples of the information economy – intelligent, self-guided, at home with technology and creative. Poster-boys and girls for the information age, hackers are at the same time a new breed of saboteurs in the world of e-commerce. By creating free software or proving that existing security programs are flawed, hackers are a thorn in the side of the corporate world. Their basic philosophies often contradict current business practices, yet employers are seeking them out in order to tap into a reservoir of knowledge that might allow their company to create the next product that will dominate the market. There is a precarious relationship

between the mainstream and the marginal in this new world of information.

There are many questions that one can ask regarding the role of hackers in our society and the basis of their motivation. For example, are hackers a rebellious group trying to change society or are they simply opportunistic nihilists who seek self-gratification by commanding power over computers? Are they the technological innovators of the future or are they impeding progress by causing the public to fear the purchase of commodities using credit cards over the Internet? Why is it that hacker groups are willing to publicize security holes instead of quietly exploiting them at will? Is it because they want to brag of their exploits or does it reflect a commitment to spreading the truth about the conflicting relationship that privacy and technology occupy in today's world? These are the types of initial questions that lead my interest in the topic of computer hackers.

The number of scientific articles written about hackers is somewhat limited which may be due to the relatively new development of this phenomenon. Although computers have been around since the post-war period, they were generally reserved for researchers until the late sixties and seventies when they made their way into the market place (Jones International 1994*). With the exception of research centres, the most common application of computers was for record management and often used only by clerks. With the expansion of the

computer's word processing capabilities, the eighties and the nineties witnessed the diffusion of computers into every type of office environment. As a result, more people had access to computers at work and the field of the personal computer blossomed[2]. The first sociological studies that focused on computers dealt primarily with the issues that resulted from automation and the changing nature of how work was being performed in white-collar occupations. With the exception of computer games, it was not until the early nineties that large segments of the population started to use computers outside of work. In the seventies and early eighties only key office workers (usually low-paid and low-valued staff) were found using computers, while today one computer per worker is the bare minimum standard in white-collar work environments. Whether it is to calculate one's taxes, to redesign a kitchen, or to catalogue recipes, computers are now used by many for personal consumption. With the advent of the Internet basic communication with extended family, shopping and research into consumer goods has made computers an even more interesting commodity for people to own. Therefore, one practical reason why there is little research on the subject of hackers has to do with the way computers were diffused slowly and recently throughout society. Computer hackers really are a new phenomenon.

---

[2] In 1981 IBM introduced its personal computer (PC) and the number of PCs increased from 2 million that year to 5.5 million in 1982. By the early nineties 65 million were being used. The cloning of IBM's machines lowered the price considerably allowing quick diffusion in the market place (Jones International 1994*).

Another possibility for the lack of research could be due to the limited computer capabilities of social scientists, in particular, sociologists. The computer underground is a relatively closed network of people and certain segments prefer not to be asked questions by outsiders. Although hackers want knowledge of computers to become more widespread, people must demonstrate a certain level of understanding of computers before attempting to question hackers on the subject. A sociologist has to have a passion for computers and an understanding of the subcultures that surround the computer enthusiasts. Furthermore, hackers have a legitimate fear of being arrested, as some of their activities are unlawful. Gaining the trust of hackers can be very difficult. Not fully understanding the technology can be intimidating to the researcher and can possibly lead to misunderstandings that limit the scope of interaction between the researcher and hackers.

Much of the literature and research that will be referred to throughout this study has taken place in the United States. There are several reasons for this, the first being that the vast majority of literature that deals with hackers is focussed on American hackers. As was highlighted earlier, the Internet is an American invention. That is not to say that other networks were not created in other countries before the introduction of the World Wide Web. Canada, France, Germany and England all had networks before the latest incarnation of

the Internet was created. There is however, a relationship that the United States has had with technological production that has not been replicated in any other country (Chomsky 1992: 82). Since the Second World War, the Americans have been at the forefront of technological creation. This is in part due to the large amounts of State subsidies that went into creating high-technology industries during the Cold War (Chomsky 1992: 21). Under the guise of national defence, the U.S. government provided much of the needed capital for research into semi-conductors, microchips, and fibre optics. Furthermore, the large middle-class of America had the disposable income needed to purchase computers and start the private consumption of this commodity before other countries. The dominance of the private market in the field of communications is also a factor in understanding the growth of the Internet in America. Where some countries attempted to maintain control over their communications networks, the private market in the U.S. allowed for new technologies to be applied without waiting for the State to debate the issues and pass regulatory frameworks (Gutstein 1998: 28-29).

It is important to note that the use of U.S. material is of little importance when discussing hackers. This is due to the fact that the subculture of the computer underground transcends national boundaries. Regardless of whether the hackers are from North America, Europe or Asia, there are common philosophical beliefs that

they share. For example, freedom of information and the freedom to circumvent barriers are important to the Chinese Hong Kong Blondes, the German Chaos Computer Club, and to the American Cult of the Dead Cow. Hackers truly are an example of a globalized culture that cuts across nation States. By defacto, this study is more of a reflection on *hackers* generally than *American hackers* specifically.

The research presented in this study is meant to highlight what hackers represent by asking and attempting to answer one pertinent question: Are hackers a social movement contesting societal constraints on technology and communication or simply a fleeting criminal subculture filled with apolitical nihilists? In order to answer this question comprehensively, this study is divided into five main sections. The first section is a review of existing literature that will be used to clearly define what hackers are and what represents the hacker philosophy. The second section will present the research questions that guide this study and the various theoretical lenses that will be applied to clarify this phenomenon. The third section explains the methodology that will be used in attempting to answer the pertinent research questions. Section four is the presentation of first hand material gathered in the hope of developing a better comprehension of the subject matter. Finally, the fifth section is a reflection on the issue of hackers and an attempt to answer the research key questions by drawing on a wealth of resources.

Chapter 2 – Literature Review

2.1 Introduction

A discussion of available literature on the subject of hackers presents some difficulties. The first is due to the recent nature of the phenomenon and the fact that very few authors have studied hackers. Of those who have written books or articles on the subject, a large number are by journalists. These accounts tend to be more sensationalistic and lack the analytical depth that a sociological analysis would present (Chantler 1995: 26). Another difficulty is due to the very organization of the activity of hacking. Since the Internet is the central tool that connects hackers, online accounts must be read and analyzed with skepticism. One must keep in mind the old adage "Don't believe everything you read", particularly regarding anything read on the Internet. Certain elements of hacking are illegal, which creates a culture of mistrust, compounded with the fact that communication through the Internet is a faceless interaction that easily allows exaggerated or minimized accounts of hacking. For example, a person might lie about their exploits in order to elevate their status, or on the contrary, they might try to conceal their criminal behaviour. Generally, whatever information is gathered via the Internet needs to be closely examined and ideally supported by an additional source,

which tends to be very difficult for the subject of hacking.[3] The purpose of this section is to review the existing literature and develop a clear definition of hacking that will be used throughout this study.

2.2 History of Hacking

Levy's work on the history of hacking is crucial to any research on the subject of hackers. He is a member of the computer underground who lived through the various periods of development and provides a detailed account of the people involved. Levy describes the first generation of hackers that developed during the 1950s and 60s as those who coalesced around the Massachusetts Institute of Technology's fledgling computer program. The Tech Model Railroad Club was the first grouping of students who had the opportunity to work on computers and who developed a cult-like fascination with the machines. They "...adopted the word 'hack' as a synonym for computer work, and particularly for computer work executed with a certain level of craftsmanship..." (Hannemyr 1997*). They were in fact the first programmers.

The second generation to develop arose during the 1970s

[3] A note on style: the accepted method of referencing the works of other authors includes the author's name, the publication year and the page number from which the quote was selected, example (Castells 2001: 48). Many of the works that will be referenced in this study are found on the Internet where texts rarely contain page numbers and often do not include the date that they were published. In cases where no date is provided on the web page, the reference will by (Jones N.d.*). The asterisk signifies that the source is from the Internet. In the *Bibliography* the web address of the source will be provided.

and consisted of hardware hackers. Part of the counterculture of the day, this second generation wanted to disseminate computers throughout society as part of a general movement towards a more egalitarian society which consisted of freer forms of communication. Hannemyr states that "what characterized the second wave hackers was that they desperately wanted computers and computer systems designated to be useful and accessible to citizens..." (Hannemyr 1997*).

The third generation of hackers are those that lead the development of computer games architecture (Levy 1994: 313). The explosive production of video games resulting from the youth market has fuelled some of the major developments in computer graphics. Building on Levy's history, Taylor argues that the fourth generation consists of those "...who illicitly access other people's computers" (Taylor 1999: 23). He also proposes that an additional group could be added to the fourth generation and that is the *microserfs* which were identified by fiction author Douglas Coupland in which he describes the workers for Microsoft in a satirical light (Coupland 1996). Taylor states that "this generation represents the co-optation of hacker skills by commercial computing" (Taylor 1999: 23).

2.3 Definition

Defining the term 'hacker' is a complex task due to the conflicting literature surrounding the subject. One definition of hacker

that is celebrated by popular non-computer related media, is a person who enters computer networks by unauthorized means, with either a malicious or relatively benign intent. Two images of hackers are proposed; the first is of the cyber-terrorist who enters in order to destroy data and the second is of the trespassing teenager.[4] The media's popular use of the term hacker blurs the distinction between various types of technologically related phenomena. For example, as Meyer notes, the media often confounds embezzlement and telephone fraud and labels it hacking simply because they both use some form of technology (Meyer 1989*).

Other than technical security manuals, most books written about hackers are done by journalists-turned-authors. A common thread throughout these books is their focus on four or five famous hackers, the two most notorious being Kevin Mitnick and Kevin Poulsen. The accounts tend to include physical descriptions of the hackers in question, their eating habits and daily routines (Hafner and Markoff 1995: 16, Sterling 1992: 61, Littman 1996: 3). The difficulty in studying this subject matter is that it has created "...a tendency to substitute overly speculative psychologising, trivia and hyperbole for substantive discussion of the broader social significance of hacking"

---

[4] Examples of news articles include:
"Hackers could threaten U.S. skies", (ZDNet News 2000*),
"Alleged CNN hacker faces more charges", (The Globe and Mail 2000*),
"Federal Cybercrime Unit Hunts for Hackers", (The New York Times 1999*).

(Taylor, 1999; 176). These accounts tend to be simplistic and paint the characters in question as either heroes or clever villains.

The first of the 'true crime' books to be released on the subject of hackers was by Stoll (1989). He was a system's administrator who detailed his activities in tracking Robert Morris, who is known as being the first person to have infected computers on a large scale with a worm[5]. Hafner and Markoff detail three hacker cases, one of which is the Robert Morris affair (1995). The two other hackers include Pengo, a West German hacker who provided the Soviets with readily available North American software, and Kevin Mitnick, the most famous hacker of all. Markoff also wrote a second book which was co-authored by Shimomura, a programmer who helped the authorities capture Mitnick (1996). Markoff was not the only journalist to write about Mitnick as Littman's first book was also devoted to this hacker (1996). Although Mitnick is currently the most 'notorious' cyber-criminal, he gained his title by eclipsing Kevin Poulsen, the subject of one of Littman's later books (1997).

The largest crackdown on hackers carried out by the United States government was detailed by Sterling (1992). "Operation Sundevil" had a large impact on the computer underground as many

---

[5] "A computer virus is executable code that, when run by someone, *infects* or attaches itself to other executable code in a computer in an effort to reproduce itself. Some computer viruses are malicious, erasing files or locking up systems; others merely present a problem solely through the act of infecting other code" (Theall N.d.*). A worm by comparison is simply a self-propagating virus.

people were sent to jail and many others quickly became ex-hackers for fear of being captured. Slatalla and Quittner report on the details of a fight in cyberspace between two rival hacker collectives, the Legions of Doom (LOD) and the Masters of Deception (MOD) (1995). Explaining the details of battle and the outcome of many months of provocations, attacks and counter-attacks by both groups, this book follows the same type of 'true crime' series as the others mentioned earlier.

Three recent Canadian documentaries have broached the subject of hackers. Zone Libre (1999), Undercurrents (1998) and The Fifth Estate (2001) have all approached the issue from the same angle, which is a focus on youths and the criminal element. A common feature of these documentaries is the interviews with youths who have brightly coloured hair and who are eager to brag about their latest hacker exploits. All three documentaries focused solely on the issue of hackers as computer trespassers.

Hollywood has also produced a variety of feature-length films and television programs that have focused on hackers. The first film was Wargames which is about a teenager who breaks into a military super-computer and nearly sets off a nuclear war with the Soviet Union (1983). Sneakers featured a team of hackers who were paid to test the security efforts of banks (1992). The film Hackers was about a group of teenage hackers who joyride though networks until

the day they must save the world from computer chaos due to a computer virus that was planted by an evil hacker (1995). The Net featured a computer programmer who had to stop a computer security firm from tricking the public into purchasing their product in order to protect themselves from a virus created by the security firm (1995). The latest film to be released is entitled Swordfish, where a brilliant hacker is forced against his will to hack into a bank on behalf of terrorists (2001). There is currently a weekly television program entitled Lone Gunmen, which features three characters previously from the X-Files television program, and documents the events of a group of middle-aged hackers (2001). All of the films and the television show present the same message, that although hackers are eccentric and do not look like they should be trusted, they are in fact ethical individuals who have superior technical expertise and simply need to be given a chance to prove themselves. All of the fictional shows, contrary to the non-fiction media, romanticize hackers and frame them as the main protagonists where the audience will undoubtedly support their efforts.

What is common in the popular media is that hacking is defined solely as unauthorized computer entry. This definition is one-dimensional and creates the impression that hacking is entirely a criminal pursuit. Raymond notes that hackers attempted to introduce the concept of cracking, "the act of breaking into a computer," as a

way to differentiate the classical hackers from the journalistic misuse of their label during the mid 1980s (The New Hacker's Dictionary. Raymond 1998; 130). Raymond goes on to state that,

> "Contrary to the widespread myth, this [cracking] does not usually involve some mysterious leap of hackerly brilliance, but rather persistence and the dogged repetition of a handful of fairly well-known tricks that exploit common weaknesses in the security of target systems. Accordingly, most crackers are only mediocre hackers" (The New Hacker's Dictionary. Raymond 1998; 130).

He explains that hackers usually know how to crack, but that this is simply one very small facet of hacking. As such, those who specialize only in breaking into networks are crackers, a subset of hackers. Furthermore cracking does not necessarily imply illegal actions. This was demonstrated in the Zone Libre documentary where groups of teenagers spent weekends building networks and then formed teams to try to crack each other's systems (Zone Libre 1999).

Taylor notes that contrary to popular notions the term hacking is still "...defined as an attempt to make use of any technology in an original, unorthodox and inventive way" within the computer underground (Taylor 1999: 15). In the same tradition Raymond defines a hacker as,

> "...1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. 2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming. 3. A person capable of appreciating hack value. 4. A person who is good at programming quickly. 5. An expert at a particular program, or one who frequently does work using it or on it; as in 'a Unix hacker'... 6. An expert or enthusiast of any kind. One might be an

> astronomy hacker, for example. 7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations. 8. [deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence *password hacker, network hacker.* The correct term for this sense is cracker..." (The New Hacker's Dictionary. Raymond 1998: 234).

What is important to note from these definitions is that hacking is not simply breaking into a computer network but involves more complex processes.

Intertwined within the history of hacking is the exploration of the phone networks. The telephone system was the first network available to everyone in North America and Western Europe. Phone phreaking is "the art and science of cracking the phone network (so as, for example, to make free long-distance calls)" (The New Hacker's Dictionary. Raymond 1998: 355). Its popularity was highest during the 1970s, before the widespread introduction of personal computers. Due to the changes in technology, phone phreaking today tends to rely mostly on stolen phone-card numbers and the mystique is quickly fading (The New Hacker's Dictionary. Raymond 1998: 355). Since computers use phone lines to communicate through, it seems natural that hackers are interested in understanding how each component of a network functions.

Another group belonging to the computer underground and is often confused with hackers are 'warez d00dz' (pronounced wares dudes). This group is interested in swapping pirated software and generally remains within the pirating community. Some warez d00dz

learn the ability to crack software encryption in order to facilitate the dissemination of wares to other pirates. Although some hackers pirate software from time to time, crackers might write some computer code and phreakers and pirates sometimes hack, these four areas generally remain separate and distinct fields of study (The New Hacker's Dictionary. Raymond 1998: 478).

Placing individuals into any one of the four categories is not a simple task as the categories are not mutually exclusive. As mentioned above, a hacker might need to crack a network to continue hacking. In some situations a hacker may use some pirated software or phreak a phone. The difference between the four can be determined by looking at the individual's principle goal. Cracking and phreaking are simple tools for a hacker, but not the challenge. For a warez d00dz the goal is to acquire a large amount of software, regardless of whether it will ever be used. A phreak, on the other hand, might never touch a computer, being completely content with the exploration of telephone networks. Given the sometimes slight distinctions and crossovers between the four groups, defining hackers can be quite difficult. However, a distinction between hackers and the other three groups does exist and that is the hacker's ability to write and implement computer programs.

Using the definition of hacker as computer programmer, two authors have significantly contributed to the study of hackers.

Hannemyr presents the argument that the hacker method of software production can, in some circumstances, produce superior products (1997*). Relying on Braverman, Hannemyr uses a Marxist analysis of the labour process involved in software development to argue that the hacker method of software creation is the direct result of the implementation of Taylorist policies by high-tech corporations. Open-source software is software that is licensed as part of the public's domain, which means that no other company can patent the software and limit other people's ability to use the program, disseminate it or even profit from it. This is the embodiment of the hacker ethic of information sharing and is known as the hacker method of software production.

Hannemyr begins with a brief history of hacking and states that in his view sensationalistic media has blurred the definition of what hacking is and has lead to the vagueness of the term. As a result, the hacker has been inappropriately defined as a nihilistic computer vandal or an entrepreneurial "techno-yuppie". Therefore, it is clear that the object of his study is the hacker as computer programmer and not the more one-dimensional network intruder.

Challenging the vision of hackers as poster-boys and girls for the free market and laissez-faire capitalism, Hannemyr argues that hackers have an accurate sense of history and understand the massive amounts of government spending which allowed the high-

tech sector to develop. He argues that hackers have been co-opted as symbols of liberalism. He proposes that the key difference between techno-yuppies and hackers is that the former revel in the glory and deterministic nature of computer technology, while the latter do not believe technology will change the world. Rather, hackers simply enjoy technology in and of itself.

Hannemyr conducted a content analysis of software programs, in which he compared hacker-created software to that of their commercial counterparts. He concluded that commercial software is developed with the goal of limiting the users' ability to modify and build on the software, essentially maintaining control, while hacker software is developed with the intention of facilitating the construction of superior software from a base that everyone can access. Essentially, hackers want to share their knowledge while commercial software developers attempt to hide their source code[6]. For hackers, the division between consumers and producers of products is illegitimate. Users should be producers and there should be more of an interaction between the two groups. Although Hannemyr admits that in some situations the development of software is not possible using the hacker method, he argues that when used the hacker method produces superior software.

---

[6] The source code consists of the most fundamental programming statements of a program and a text file which details how the program is constructed.

Following the same definition of a hacker, Raymond pleads the case for open-source programming. A case analysis of his creation of the fetchmail program is used in order to support his theory that open-source, or the hacker method, of software production is superior to the corporate model of development ("The Cathedral and the Bazaar". Raymond 1998*). He introduces two unique concepts to distinguish the models; the cathedral, which is the corporate model based on the notion that a few special people will carefully design and craft a structure while keeping it hidden until the end of production; and the bazaar, the community oriented model based on inviting everyone to contribute in the production process. Based on the traditional view of hackers-as-programmers, Raymond's mixture of liberal and anarchist viewpoints are reinforced by the example of Linus Torvalds, the creator of the Linux kernel[7]. The central element to the bazaar method is that the more people that have the opportunity to use a program, the more likely it is they will be able to spot errors and provide a remedy. This not only reduces the time needed to create software, but it can also lead to improvements on the design not originally envisaged. The central difference between the cathedral

[7] A kernel is the most basic part of a programming language. Torvalds is one of the most celebrated hackers-as-programmers in the world. The operating system that he created over the period of a few years with the help of many other hackers, Linux, is the operating system of choice amongst hackers and the anti-Microsoft group. This operating system is available for free on the Internet and companies such as Canada's Corel Corporation have begun making a profit selling user friendly versions to the public.

and the bazaar is the bazaar's reliance on open communication with users and the treatment of them as peers.

An example of the bazaar concept of computer programming can be found in a paper by Raymond. This paper is intended for a programming audience and contains highly technical descriptions of the problems Raymond encountered leading him to create the "fetchmail" program ("The Cathedral and the Bazaar". Raymond 1998*). His methodology for this experiment was based on four key activities; he released copies of the program early on in the production stage; he re-released revised versions often and added everyone who contacted him about the program on his release list; he sent out invitations to these people to participate in the project; and, he listened to all of his users and inputted the changes they suggested and the patches[8] they produced. People wishing to successfully adopt the bazaar style of programming according to Raymond, must begin the project and have the community build on it, must present a "plausible promise" and must be good communicators ("The Cathedral and the Bazaar". Raymond 1998*).

Raymond admits that there are problems that hamper the bazaar method. These are the "legal constraints of various licenses, trade secrets, and commercial interests" ("The Cathedral and the Bazaar". Raymond 1998*). Regardless, he continues to theorize that

[8] A patch is few lines of coding that is introduced into an existing program to remedy a problem.

the open-source method could overcome the commercial software development simply because the talent pool available to work on a bazaar type project is much larger than the talent pool that a single company is able to afford.

There is no better way to demonstrate the profound effect that the hacker open source software (OSS) is having on commercial developers than through an examination of a leaked memorandum from Microsoft. Microsoft is seen as the arch enemy of hackers and vice-versa. Many argue that the way Microsoft gained their prevalence in the marketplace was not necessarily by developing superior products, but rather by their ingenious licensing schemes (Wasserman 1998*). "Open Source Software: A (New?) Development Methodology" (Vallopillil 1998*) is an internal strategy memorandum on the possible responses that Microsoft could take regarding Linux, an OSS product and a major competitor, as well as the general OSS phenomena[9]. The document makes several key arguments as it begins with a short history of the open source community and an analysis of various open source projects that have been highly successful. The two elements that worry Microsoft most are the

[9] The document was leaked to Raymond who is well known within the open source/hacker community. In Raymond's comments prefacing the memo he states, "Microsoft has publicly acknowledged that this memorandum is authentic, but dismissed it as a mere engineering study that does not define Microsoft policy" ("Open source Software: A (New?) Development Methodology." Ed. Raymond1998*). Raymond argues however that the document should be taken seriously since the people listed as contributors to the document hold high positions within the Microsoft hierarchy.

reduction in revenue from OSS and the superior quality of work. The author of the paper states,

> "OSS [open source software] poses a direct, short-term revenue and platform threat to Microsoft, particularly in server space. Additionally, the intrinsic parallelism and free idea exchange in OSS has benefits that are not replicable with our current licensing model and therefore present a long term developer mindshare threat" (Vallopillil 1998*).

The author notes that there is a growing anti-corporate political current which is challenging commercial software development. The effects of these sentiments on consumers means that "...OSS evangelization scales with the size of the Internet much faster than our own evangelization efforts appear to scale" (Vallopillil 1998*). The author is admitting that Microsoft's advertising campaigns are not strong enough to fight a grass-roots hacker camping as, "...FUD tactics can not be used to combat it" (Vallopillil 1998*).[10] Here the sheer dedication of the OSS community becomes problematic to commercial developers because of an ideological belief in using software derived from the free exchange of information. The motivation to increase profit by lowering production costs also becomes problematic for commercial development which finds much of its revenues from lucrative licensing agreements (Weston 1998*). The more stable software is proven to be, meaning it does not

[10] The reference to FUD (Fear, Uncertainty, Doubt) is a standard Microsoft tactic (but not reserved solely to them) of attacking competitive software as "...scare-mongering is used via 'gossip channels' to cast a shadow of doubt over the competitors offerings and make people think twice before using it" (Irwin 1998*).

malfunction, the more people are willing to use it as an inexpensive alternative.

The final element that is apparently troublesome to the author of the paper is that, "The ability of the OSS process to collect and harness the collective IQ of thousands of individuals across the Internet is simply amazing" (Vallopillil 1998*). Understandably, commercial developers cannot keep on retainer an unlimited number of programmers to perfect products. This presents disadvantages to commercial vis-à-vis OSS projects. The author cites Raymond's arguments for the superior parallel debugging that takes place in open source projects that cannot be replicated by commercial companies.

In an insightful analysis the author suggests that the strategy that Microsoft should adopt is to attack the process of open source development rather than waste its energy attacking a single company or product. Instead of fighting Linux, a symptom, Microsoft has to attack open source development, the cause. Accepting that the defeat of the open source community is highly improbable, if not completely impossible, the author suggests changing Microsoft's commercial process by adopting certain open source methods. Three of the more interesting suggestions by the author include; 1) capture parallel debugging through more liberal code licensing to organizations such as universities, 2) provide entry level tools for low cost or for free in order to "generate a common skillset/vocabulary tacitly leveraged by

developers," and 3) distribute parts of the source code to "generate hacker interest in adding value to MS-sponsored code bases" (Vallopillil 1998*).

The importance of this leaked memo cannot be over emphasized. Microsoft is the largest software developer in existence and is a market leader. One could argue that if a commercial developer the size of Microsoft is afraid of the competition that the open source/hacker community poses, then the entire field of commercial software must also be closely studying this tangible manifestation of hacker ideology.

2.4 The Hacker Ethic

There is a great deal of debate surrounding what the hacker philosophy actually is or what it should be. There are four key texts that describe the hacker ethic. Two are historical works and two are recent elocutions of the ethic.

In the first historical text, Levy argues that there are six components that comprise the hacker ethic. They include;

> "1) Access to computers – and anything which might teach you something about the way the world works – should be unlimited and total.
> 2) All information should be free.
> 3) Mistrust Authority – Promote Decentralization.
> 4) Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race or position.
> 5) You can create art and beauty on a computer.
> 6) Computers can change your life for the better"
> (Levy 1994; 40-45).

Another historical text, often cited as one of the first hacker texts to describe the ethic, was "The Hacker's Manifesto", written by a hacker who calls himself "+he Mentor" and was released in 1986 (+he Mentor 1986*). The text begins by explaining the alienation and boredom that hackers face in school due to the lack of challenging material. Hacking is about curiosity, the search for knowledge and figuring out how things work. +he Mentor makes reference to the community of hackers and the sense of belonging that they find through their computer networks and phone lines.

A more recent and succinct definition of the hacker ethic comes from Raymond. It is defined as,

> "1. The belief that information-sharing is a powerful positive good, and that it is an ethical duty of hackers to share their expertise by writing free software and facilitating access to information and to computing resources wherever possible. 2. The belief that system-cracking for fun and exploration is ethically OK as long as the cracker commits no theft, vandalism, or breach of confidentiality" (The New Hacker's Dictionary. Raymond 1998: 234).

In another recent text, Newby proposes the "Hacker Code," which is as follows;

> "Preamble: Hackers are diverse, from all cultures and backgrounds. Every hacker is unique, yet we all share some characteristics. While not every hacker follows this Code, many believe it is a fair description of our shared traditions, goals and values.
> 1. Hackers share and are willing to teach their knowledge
> 2. Hackers are skilled. Many are self-taught, or learn by interacting with other hackers.
> 3. Hackers seek knowledge. This knowledge may come from unauthorized or unusual sources, and is often hidden.
> 4. Hackers are tinkerers. They like to understand how things work, and want to make their own improvements or modifications.

> 5. Hackers often disagree with authority, including parents, employers, social customs and laws. They often seek to get around authority they disagree with.
> 6. Hackers disagree with each other. Different hackers have different values, and come from all backgrounds. This means that what one hacker is opposed to might be embraced by another.
> 7. Hackers are persistent, and are willing to devote hours, days and years to pursuing their individual passions.
> 8. This Code is not to prescribe how hackers act. Instead, it is to help us to recognize our own diversity and identity.
> 9. Every hacker must make his or her own decisions about what is right or wrong, and some might do things they believe are illegal, amoral or anti-social.
> 10. Hackers' motivations are their own, and there is no reason for all hackers to agree.
> 11. Hackers have a shared identity and many shared interests.
> 12. By reading this Code, hackers can recognize themselves and each other, and understand better the group they are a part of" (Newby N.d.*).

The sources of Newby's code are threefold; the Hippocratic Oath, Asimov's Laws of Robotics and The Hacker's Manifesto by +he Mentor ("The Hacker's Code: H2K". Newby 2000). Newby uses the roots of the physician's Hippocratic Oath which expresses that no harm should be done to others and that teaching future practitioners is paramount. As is frequently the case in the hacker subculture, Newby makes reference to a work of science fiction. In Asimov's book, the *Zeroth Law* states that a robot may not injure humanity (Asimov 1990: 424). The argument that Newby is trying to make is that hacking is supposed to be beneficial to society rather than being motivated by private profit or destructive purposes. All four definitions have two principle themes, the first is the free sharing of information and the second is the justification for breaking into computer networks.

Open access to information relating to software programs is a core belief in the hacker ideology. The hacker open-source method is in contrast to closed-source coding in which the only people that have information about the building blocks of a program are the programmers of the particular software or the company that has purchased a license from the software producer. The proponents of open-source coding believe that society as a whole benefits when the source code is free for anyone to build on. Open-source coding is in direct conflict with the formula used by the business community to make a profit from knowledge-based work. From the business perspective, hiding the intellectual underpinnings of a program is necessary in order to protect the investment made in the research and development of the software. In addition, licensing other companies with the right to use the intellectual products of a code is a lucrative element of the software market.

Himanem applies the Weberian concept of the Protestant work ethic to the phenomena of hackers in order to explain the hacker ethic (Himanem 2001: 8). He argues that the hacker ethic is a competing ethic that is fuelling the growth of the information society. Key to his argument is that hackers are promoting an open model of learning and development. By using the analogies of the academy of science and the monastery, Himanem argues that the pre-hacker method of software development closely resembled the monastery in

which learning was a one-way process between master and disciple. In contrast, the hacker method is more connected with the academy of science and its reliance on synergy between students and faculty and the need for peer evaluation of work.

Reflecting on Raymond's earlier definition, another key element to the hacker ethic is the justification of unauthorized entry into networks. Here, the ethical line becomes somewhat blurred. For example, if hackers believe that it is ethically acceptable to enter unauthorized computer networks, does that imply a belief that all information should be accessible to everyone and anyone? Does this include medical records, employment records, credit records? Surprisingly, hackers are in fact some of the most ardent supporters of privacy on the net[11]. This contradiction between their beliefs and their activities is somewhat confounding. A person travelling online is likely to notice that hackers rarely use their birth name as their online handle. Just like short-wave radio enthusiasts, hackers have adopted the use of aliases online in order to protect their identity. The choices of online handles often come from science fiction novels or clever references to technology[12]. An example of the fervent support for

---

[11] The Electronic Frontier Foundation was started by Mitch Kapor (founder of Lotus Development Corporation), Steve Wozniak (co-founder of Apple Computers) and writer John Perry Barlow. The organization is supported by the hacker community and has lead a campaign for online civil liberties and privacy since its foundation in 1990.

[12] 'Count Zero' from William Gibson's Neuromancer or 'Phiber Optik' are examples. Some come from political satire such as 'Emmanual Goldstein' the owner of 2600: The Hacker Quarterly, who's handle is in reference to the fabricated state enemy in George Orwell's 1984.

privacy was the use of *cookies* and the way that hackers uncovered the issue[13]. Hackers were the first to point out the use of cookies to the public. Cookies are software packets that allow an Internet site to track the subsequent sites a person visits (L'Internaute.com N.d.*). The information collected serves as consumer data, which are then sold to a variety of companies for marketing purposes. Once knowledge of cookies became widespread and circumvention techniques developed by hackers made them useless, the computer industry developed computers with the Pentium III processors that left the chip's serial number on every site to track every surfer's habits (Seminerio 1999*). Hackers were again the first to publicize this fact and to develop circumvention techniques for the new technology. The interest in online privacy reflects the view of the computer underground that commercial interests and government censors have no place on the Internet.

As was noted by British hacker Wignall, hackers have their own interests at stake in keeping the Internet safe from malicious hackers (Wignall 2000). The medical information and employment records kept on the net of Mr. X or Ms. Y are not different for hackers and non-hackers. Computer hackers understand that the Internet is in fact a very unsecured place and, as such, argue that by providing

---

[13] Examples include the article by Canlas (1997*) in the Happy Hacker Digest and Haselton and McCarthy's web site which allows users to input the URL of various sites, and have forwarded back to them their cookie ID information for any site that they have visited that stores user-ID cookies (Haselton and McCarthy N.d.*).

examples of the holes that allow people to break into various networks, they will in essence be sounding alarm bells for companies and governments to invest more in protecting the data that is transferred through network lines[14].

One of the key arguments made by hackers is that networks are currently unsecured to the point that it should qualify as negligence on the part of system administrators and the companies that produce network software (Steele 2000). Jordan argues that hackers and the computer security industry are engaged in a battle of analogies. The analogy that the computer security profession and police organizations like to use is that hackers are essentially breaking and entering, just like a burglar or vandal would do to a house or business (Royal Canadian Mounted Police N.d.*). Accepting this analogy, most people would reason that hackers are to blame for computer intrusion and that it is impossible to rationalize this behaviour. Thus, if we as a society do not accept this behaviour offline, there is no reason it should be tolerated online.

On the contrary, hackers prefer the analogy of a person who leaves their keys in their car, with the engine running and the doors unlocked (Taylor 1999: 147). Many of people would accept that the

---

[14] In an interview recently convicted hacker Raphael Gray, a.k.a. Curador, explained that he was posting credit card numbers on the Internet in order to bring attention to the lax security on certain sites. He stated "There are a lot of people out there who won't even safeguard their own safety, let alone the safety of their customers. At the end of the day, it's the fault of these companies" (Gray as quoted by Public Broadcasting Station N.d.*).

owner of the car was in fact partially responsible for the theft of their vehicle. Hackers argue that the security problems on the Internet are the fault of the companies that do not suffer any consequences when they sell faulty software laden with security holes. The hacker ethic allows for the unauthorized entry into networks, with the limitation that confidential data should not be destroyed nor used for nefarious purposes. Respect for the limitations to information sharing is crucial to the hacker ethic and the status a hacker holds in the hacker hierarchy.

Adherence to the hacker ethic plays a significant role in what position a person holds in the hacker hierarchy. To better illustrate the hacker hierarchy the more popular terms in the computer underground need to be defined, including; elite hacker, dark-side hacker, white hat hacker, script kiddies, code grinders and wannabes.

The term *elite* hacker is rather obvious, as the reference is the same in mainstream society, in that the hacker is one of the best. Elite hackers are often part of elite groups where membership is acquired by providing proof of an exceptional hack. *Legions of Doom* or *Cult of the Dead Cow* are infamous hacker collectives that are examples of elite groups. When a hacker gains entrance to these underground groups they become gods in the hacker subculture – automatically gaining respect from others because they have earned

the privilege to be part of the group[15]. Being an elite hacker does not necessarily indicate whether a person carries out malicious hacks or not. Two types of elite hackers exist within the hierarchy. There is the *dark-side* hacker "a hacker who uses his or her talents for malicious or criminal ends" (McFedries 2001*). The antithesis of this is the *white hat* hacker who will alert a system's administration when they find vulnerabilities.

A *code grinder* is someone who is a computer programmer, but not a hacker. The key difference is their lack of adherence to the hacker ethic or philosophy. A code grinder is also known as a *suit*, referring to the typical business attire that a regular programmer would wear when working for a mainstream firm (The New Hacker's Dictionary. Raymond 1998: 115).

A *wannabe* is actually a somewhat-positive term. It means a person who is on their way to becoming a hacker. They have the correct philosophy, but they do not possess the technical ability to be classified as a hacker. Once they have developed their technical ability they will move up the hacker hierarchy. A closely related term is a *script kiddy*; a person who downloads hacker software for cracking networks and applies them to his or her target. Script kiddies lack the

[15] For example, the Cult of the Dead Cow's site includes a 'Team Bio' which states the person's handle, when they became 'members' of the group and some type of title (ex. The Death Vegetable • member since December 1990 • Minister of Propaganda; Oxblood Ruffin • member since April, 1996 • cDc's Foreign Minister) (CdC 2001*).

technical talent to write their own code, which is why they depend on programs written by others. Because of their reliance on using other people's programs instead of learning how to create them themselves, these people are seen as not having the true hacker ethic. It is generally assumed that these people are young teenagers, new to the scene of hacking (Oxblood in Zone Libre 1999).

These terms are important as they demonstrate the hierarchy that exists within the computer underground. This hierarchy is based on technical ability and living by the hacker philosophy. An elite white hat hacker is the truest embodiment of hacking as they have the technical abilities and the proper world outlook. Such an elite hacker will not want to share all of his or her knowledge with a script kiddy because the hacker philosophy requires a person to pass through different levels of training to prove their worthiness. To gain entry into an elite hacker collective, a person must have a good reputation within the hacker community and a particular expertise sought after by the group.

Script kiddies are looked down upon in the community. This is because it is thought that many of the high-profile cases of web defacements and the destruction of data, either intentionally or inadvertently, are caused by these people. It is felt that script kiddies do not have an appreciation of a hack and lack the technical abilities needed to prevent damage. During interviews, elite hackers often

lament the fact that script kiddies come online and try to pry information from them (Oxblood in Zone Libre 1999).

The hacker ethic of information sharing is limited by the belief in a meritocracy within the underground. Although more advanced hackers are often willing to teach others, they impose restrictions that ultimately benefit the community and attempt to leave the net safe from incompetent or malicious script kiddies.

2.5 Organizational Theory

There are two particular studies that provide insight into the social organization of the computer underground. In the first, Meyer attempts to apply the typology of deviant organizations, developed by Best and Luckenbill, to the computer underground (Meyer 1989*). This criminological typology is based on four principle elements: mutual association, mutual participation, division of labour and extended organization. The higher the degree of development displayed in each of the elements translates into a higher level of organizational sophistication. Five categories of organizations then follow: loners, those who act alone; colleagues, those who "associate with fellow deviants"; peers, those who associate with each other but also perform their deviance together; mobs, where there is a high division of labour; and finally formal organizations, which encompass the last three definitions but also add to them the fact that deviant "activities extend over time and space" (Best and Luckenbill 1982; 24-

25 as cited by Meyer 1989*; 35). Meyer's hypothesis is that members of the computer underground, contrary to the media's portrayal as loners, actually form a loose-knit community. He makes a clear distinction between three types of computer deviants which are the subject of his analysis; hackers, as computer intruders, phreakers and pirates (e.g. warez d00dz). What Meyer classifies as a hacker in his study closely resembles what is known as a cracker today, although he uses the term cracker in reference to the more skilled 'warez d00dz' that break anti-copy encryption software. Meyer's concluding argument is that as long as hacking remains at the current level of sophistication with the limited means of support and weak ties between individuals, the activity will remain a "transitory and limited 'criminal' enterprise" (Meyer 1989*; 79-80). He ends by saying that there is no evidence supporting the notion that the computer underground is growing and, based on his analysis "it is not likely to do so on a large scale"[16] (Meyer 1989*; 80). Meyer's contribution to the study of hackers is found in his theoretical framework in understanding hackers as members of a community.

From a slightly different angle, Rosteck employs the theory of social movements to analyze the hacker phenomena as developed

[16] More recent data has proven this to be false as the number of organizations dedicated to hacking have grown and that the number of unauthorized computer intrusions have also grown dramatically. Hacker attacks have more than tripled in the past two years as "The government's Computer Emergency Response Team reported about 5000 cases of corporate hacking in the United States in 1999 and more than 17,000 cases in 2000" (Zetter 2001*).

by Stewart, Smith and Denton (Rosteck 1994*). Rosteck's definition of hackers is rather broad as "...hackers are defined as computer enthusiasts who have an ardent interest in learning about computer systems and how to use them in innovative ways" (Rosteck 1994*). Rosteck attempts to limit the subject matter by eliminating malicious hackers who try to destroy data from the definition. The definition is vague enough to encompass both those who break into computer networks and those that write computer programs. Rosteck's ethnographic approach relies on a content analysis of hacker journals. This type of analysis is limited by the difficulties in entering the underground bulletin boards and precludes the discreet observation of postings. Regardless, the variety of journals reviewed still demonstrates a very thorough analysis of the material written by hackers. Rosteck's argument is that hacking can be interpreted as a protest against corporations and the State, which both try to silence computer enthusiasts. Rosteck argues that hackers conform to the six requirements for the existence of a social movement, being;

> "1) A social movement has at least minimal organization, 2) A social movement is an uninstitutionalized collectivity, 3) A social movement proposes or opposes a program for change in society norms, values, or both, 4) A social movement is countered by an established order, 5) A social movement must be significantly large in scope, and 6) Persuasion is the essence of social movements" (Rosteck 1994*).

Rosteck's argument that hackers comprise a social movement is an important addition to the multitude of theoretical frameworks that have been used to analyze the computer underground.

2.6 Hackers and the Security Industry

Due to the nature of activities that hackers engage in, a look at the security industry and the way hackers relate to it is crucial. Taylor focuses on the relationship between the computer security industry and hackers.

> "As a broad simplification, computer cognoscenti are split into two camps: those who either come from or are prepared to co-operate with the computer underground and those to whom the computer underground is an anathema. Borrowing from the argot of the cold war, I describe the two ends of this spectrum of opinion as the hawkish and dovish camps. Hawks advocate little or no co-operation: the computer underground should be punished in the courts. The doves, in contrast, argue that hackers represent an important stock of technical knowledge that society should not prematurely isolate itself from by adopting a 'punish first, ask questions later' approach" (Taylor 1999; xi).

Taylor explains that knowledge created by hackers is not utilized in the computer security field because, "...it interferes with their boundary-forming project that centers upon attempting to define the difference between a hacker and a computer professional" (Taylor 1999; 118). Taylor points to their conception of property as being the key difference between the security professional and the hacker (Taylor 1999; 135). He describes the professionalization process that some hackers attempt and the difficulties they face when leaving their computer underground to cross over to legitimate work. The process

of professionalization has also lead to the movement to criminalize hacker activity (Taylor 1999; 122). The importance of Taylor's work is the highlighting of the process of defining a hacker versus a legitimate computer security programmer.

Following the same theoretical framework, Taylor teamed up with Jordan to apply an interactionist perspective to explain the formation of a community identity for computer hackers (Taylor and Jordan N.d.*). Their subject matter is narrowly defined as hackers as unauthorized computer intruders and they discuss the relationship between the hacker community and the computer security industry. This study is partially a qualitative analysis of hacker case studies in the form of interviews with hackers and partially a quantitative analysis of a survey completed for the purposes of the paper. Jordan and Taylor attack the popular notion of a hacker as an independent obsessed loner based on the fact that there is a well-defined online network with magazine publications and online bulletin boards. In the concluding analysis presented by Taylor and Jordan, they ask how external boundaries are constructed and maintained. Their answer to this question is that hackers create and maintain their community image through the interaction with the computer security industry. It is this interrelationship with the security industry that confirms that hackers are not in fact a self-constituted community. The two sides have a precarious relationship because of the need to create a

working definition so that they can differentiate themselves from each other. Taylor and Jordan note the various cases in which ex-hackers are hired as security consultants. They describe the key difference between the untouchable elements of the hacker community by the security industry are those that have the label of criminals.

A recent phenomenon highlighted by the media has been the hiring of hackers as computer security specialists (Ludlow 1999*). There are two ways that hackers have been integrated into legitimate security; the first is as hackers who form their own hacker-run firms and the second is as employees of an existing legitimate non-hacker-run security company. Two examples of hackers who created their own hacker-run firms are the ComSec, which was started by Chris Goggans[17], and L0pht Heavy Industries which has just integrated with @Stake, a legitimate computer security firm.

There is no shortage of articles that detail the second way hackers are integrated into the security field, namely through

---

[17] Also known online as Erik Bloodaxe, an ex-member of Legion of Doom (LOD). Slatalla discussed briefly the experience of Goggans when he started ComSec (Slatalla 1995). Goggans was member of the elite hacker group LOD. The group used to organize phone bridges, long-distance teleconference calls (for free) between hackers. During one of those telephone bridges someone from the inner city of New York with a heavy hip-hop accent began to speak. Another hacker immediately shouted a racist epithet at which point everyone hung up. Those that were from New York decided to form their own hacker group called Masters of Deception (MOD), and this group attempted to outshine LOD by harassing the other group's members. Goggans had recently launched his own computer security firm when all of this occurred. The MOD members began harassing Goggans at his company by turning the phones into a payphones, which meant that every time he tried to make a call an automated voice would ask for a quarter to be inserted. They also began listening in on conversations, interrupting at will and disconnecting calls. The ComSec case is the first recorded time of a hacker becoming a security consultant and highlights some of the dangers involved in crossing other hackers.

employment in non-hacker firms. IBM and Ernst & Young, arguably the furthest companies from any type of counterculture or hacker underground, have tiger teams that include hackers, which they rent out to many of the biggest companies in the world to test their own networks (Glasner 1999*). Pricewaterhouse Coopers has a tiger team of hackers that is part of their Enterprise Security Solutions Practice and released a document to customers on how to hire a professional hacker (The Guardian 2000*). It is not uncommon for security specialists to give advice as to what to look for when hiring a hacker. The helpful hints are nothing more than standard business practices such as confirming references, noting the person's credentials (school is not necessarily the only acceptable credential), forming a detailed work plan, etc. Those that argue that hackers should not be hired state that a good computer security specialist should have certifications such as being an Information Systems Security Professional (CISSP) or an Information Security Auditory (CISA) (Merritt 2000*). However, many companies are forgoing the certifications because of a belief that some hackers are better than certified security specialists. It could be that the training dulls the edge that gives hackers the ability to think innovatively about security and programming issues. When discussing the topic of hiring hackers, authors make reference to the hiring of an "ethical hacker", which is an attempt at differentiating between the media's folk devil and the

common version found by most employers (Nair-Ghaswalla 2000*; Callaway 1997*)[18].

2.7 Conclusion

In order to define a person as a computer hacker two important elements must be present; their technical ability as well as their philosophical outlook. Hacking is not simply breaking into networks. A study that uses this definition as its basis limits itself to a very small segment of the hacker community. The definition of a hacker must include the production of programs as well as the use of circumvention techniques. Just as the bumper stickers of the Electronic Frontier Foundation state "Coding Is Not A Crime", it follows that not all hackers are criminals. Networks can be created and people can play games trying to break into them as is done at virtually all hacker conventions. This study will employ the definition of hacker as a passionate programmer who enjoys overcoming or circumventing technological limitations and has adopted the hacker ethic. This definition includes those who enter networks through unauthorized ways but excludes those who are mislabelled hackers

---

[18] The private market is not the only employer searching for new talent. Governments have now begun to openly recruit and use hackers. The 1980s movie *Wargames,* about the army joining forces with a young teenage computer geek to save the world from World War III foreshadowed today's reality. It is not surprising to find a speaker at H2K being an ex-CIA agent (Steele 2000) nor is it odd to see a high-ranking FBI agent make a presentation at Defcon IV (Defcon.org*). Many hacker celebrities such as Dark Tangent, Se7en and Death Vegetable have announced their new jobs as a security consultants by passing out business cards at Defcon (Lange 1996: 4). While the FBI began recruiting and tabulating files on individuals since the very first hacker conference, now they openly hand out recruitment forms (Jackson 2000: 1).

simply because their crimes involve computers. It is this dual definition of programmer and an adherence to the hacker ethic which I believe offers the most accurate portrayal of what hackers are today.

Chapter 3 – Theoretical Framework

3.1 Introduction

The definition that I have adopted for computer hackers includes both the ability to produce open-source software and the cracking of networks. Part of what is lacking in previous research is an analysis of the hacking community that includes both elements of this definition. This section highlights the research questions that have motivated this study and presents a variety of theoretical lenses which will be of use in answering them. These theories have been derived from a variety of studies that focus on the hacker phenomena as well as research in unrelated areas that are nonetheless applicable to this study.

3.2 Research Questions

After careful review of existing literature on the subject of hackers there are questions remaining that have yet to be adequately answered, including; why there is a growing interaction between the hacker community and mainstream software companies and governments? Why do hackers seem to want to engage mainstream society in a meaningful dialogue about technology? With their beliefs in the transferring of knowledge, are hackers a democratizing force? What is the relationship between the hacker community and the media? Are hackers simply deviants or do they represent a rebellious

group? The first step to answering these questions is to understand the background in which hackers operate: the information economy.

3.3 The Growth of the Information Society

Hackers are inextricably linked to the information economy. Three key authors have undertaken the task of deciphering what the information economy is and how it differs from the traditional economy. The first author is Touraine who attempted to describe the changes affecting industrial societies (Touraine 1969). He replaced the term 'post-industrial' with 'programmed' society to reflect what he felt was the increasing control and organized nature of the new society (Touraine 1969: 7). Touraine also used the concept of technocracy to describe a new form of power which was the reliance on managers rather than owners to make major social decisions (Touraine 1969: 7). The central difference between an industrial and a programmed society is that the conflict resides between managers and those being managed rather than between owners and labourers. Those in power are the technocrats who are not technicians but rather managers. Power resides not in economic production but rather, in the ability to direct culture and knowledge. Touraine's theory is in accordance with Hannemyr's theory of how hacking as a method of software development resulted from the introduction of Taylorist control methods by managers in high-tech companies.

Following Touraine, Bell's work focused on the linear passage of society through three distinct periods: pre-industrial, industrial and post-industrial (Bell 1973: xci). For Bell, the way knowledge is treated is the central element to a post-industrial economy and two in particular are of importance to the study of hackers: the spread of a knowledge class and the economies of information. The knowledge class is composed of technicians and managers and represents the fastest growing group in society. The economies of information presents a sort of paradox since knowledge is a collective good, but becoming more and more the object of private corporate control (Bell 1973: XCIV-XCVI). One final element to draw from Bell is that the growth in the importance of knowledge has lead to a new dominant class of people, namely, those able to control the flow of information (Bell 1973: xcv). Bell's analysis is complemented by Raymond's view that hackers represent an attack on the secretive use of new information for the sole purposes of profit. Open-source coding is a direct affront to the patenting and limitations of use agreements that are becoming more and more the norm.

Castells is the latest sociologist to produce a seminal work on the subject of the information economy. He contributes to the sphere of sociology by explaining some of the structural changes in modern day society that have resulted from emerging technologies (Castells 1996). He uses the term "informationalism," as opposed to

post-industrial or programmed society, in order to illustrate the importance of information, not only as a tool in the new economy but also as a commodity (Castells 1996: 17). What differentiates today's western economies from yesterday's is the central importance that the production of knowledge and information plays. While Touraine and Bell include the service industry in their analyses of the post-industrial economy, Castells argues that it is specifically the industries that produce information that are at the core of the transformations observed in today's society. He uses an analysis of corporations, which he describes as network enterprises, to explain the profound impact of organizational changes that have been facilitated by the advent of new communication technologies. Castells makes it clear that globalization and the international division of labour has occurred due to organizational changes rather than arising in a mechanical fashion from new technology, although these new technological developments have facilitated and made possible the intensification of these social changes (Castells 1996: 168-69). Castells notes the advances in communication technologies which gave rise to greater power of managers over employees to control work and its processes (Castells 1996: 168-69). The key element of Castells theory that relates to hackers is the way in which "networkers" have grown in power in relation to other workers due to the nature of their work (Castells 1996: 201, 203-204). Hackers and programmers are part of

a new powerful group that occupy a central position to the new economy of information.

The importance of Touraine, Bell and Castells is that they all argue that society has entered a new organizational state. Whether it is called the programmed, the post-industrial or the information society is of little importance. They agree on two principle issues; that the changes are the result of political influences and these changes have been made possible due to technological advances. Although they do not speak directly about the development of the hacker, all three argue that technologically proficient people will grow in power. The value of these theorists' work is that they present the backdrop in which hackers operate and provide a theoretical basis for understanding the complex relationship that hackers as technologically proficient people have with the rest of society.

3.4 The Relationship Between Hackers and the Media

Cohen's concept of a moral panic is useful in understanding the relationship between hackers and the media. He states that a moral panic occurs when,

> "A condition, episode, person or group of persons emerges to become defined as a threat to societal values and interests; its nature is presented in a stylized and stereotypical fashion by the mass media; the moral barricades are manned by editors, bishops, politicians and other right-thinking people; socially accredited experts pronounce their diagnoses and solutions; ways of coping are evolved or (more often) resorted to; the condition then disappears, submerges or deteriorates and becomes more visible" (Cohen 1980; 9).

Cohen's analysis results from a case study of two 1960's youth cultures, the Mods and the Rockers. There are three key processes in the creation of a moral panic; exaggeration and distortion, prediction, and symbolization. The media exaggerates the effects and frequency of a phenomenon and then offers predictions of when it might happen again. This, in turn, reinforces the urgency that is required for the authorities to act immediately in order to safeguard society. Cohen argues that the third process is "symbolization" or the process of making neutral words symbolize complex ideas and emotions and has three elements. These elements are; "...a word becomes symbolic of certain status (delinquent or deviant); objects symbolize the word; the objects themselves become symbolic of the status..." (Cohen 1980; 40). Cohen also argues that "another highly effective technique of symbolization [is] the use of dramatized and ritualistic interviews with 'representative members'..." (Cohen 1980; 42). In the creation of a moral panic, a consistent theme is that the indignation the media professes contrasts sharply with the public perception of the situation (Cohen 1980; 66). The use of Cohen's concept of moral panic can be of use in understanding the relationship between hackers and the media.

3.5 Hacking as a Method of Cultural Adaptation

Merton's functionalist approach to explaining issues of deviance in society relied on the premise that deviance stemmed from

a conflict between society's culture and its social structure (Merton 1957; 122). When a discrepancy develops between the socially valued goals and the socially accepted methods of achieving these goals, deviance occurs. It is necessary to note that deviance is not an innate pathological character flaw, but rather stems as a direct consequence of the conflict of culture and structure. Merton developed a typology to explain methods of cultural adaptation in society. Relying on the role that cultural goals, the "purposes and interests, held out as legitimate objectives for all or for diversely located members of the society," and institutional norms, "the acceptable modes of reaching out for these goals," Merton posits five distinct types of individual adaptation (Merton 1957; 132-133).

Modes of Adaptation	Culture Goals	Institutionalized Means
Conformity	+	+
Innovation	+	-
Ritualism	-	+
Retreatism	-	-
Rebellion	+/-	+/-

Within the above table, (+) signifies the acceptance of either the goals and means and (-) signifies the rejection (Merton 1957; 140). In the *Rebellion* category, the (+/-) signifies the rejection of existing goals and means and their replacement with other goals and means.

The majority of society adapts by conforming to the goals and the means at their disposal. The innovator places more emphasis on the ends and thus rejects the means and accepts the goals.

Examples of innovators are criminals who accept the cultural goals (i.e. material wealth) yet reject the institutionalized means. Ritualism refers to the type of individual who adapts by the "...abandoning or scaling down of the lofty cultural goals of great pecuniary success and rapid social mobility to the point where one's aspirations can be satisfied" (Merton 1957; 150). The retreatist by contrast, not only rejects the goals but also the means. Drug addicts and the like who disengage completely from society fit into this category.

The final type of adaptation in Merton's typology is that of the rebel.

> "This adaptation leads men outside the environing social structure to envisage and seek to bring into being a new, that is to say, a greatly modified social structure. It presupposes alienation from reigning goals and standards. These come to be regarded as purely arbitrary" (Merton 1957; 155).

Merton's concept of cultural adaptation will be useful in answering some of the questions asked in this study.

3.6 Conclusion

As has been demonstrated, many questions abound, including how to explain why hackers want to talk to software companies and how should the hacker phenomena be interpreted? Are hackers a rebellious group who are challenging existing social structures and if so, what is their social project? Are hackers a unified group or are there conflicting interests within the underground community? Can hacking be interpreted as a democratic force or is it

merely an opportunistic pastime for nihilists who've adopted progressive discourse for the purposes of legitimizing their activities? Touraine, Bell and Castells were chosen for their ability to give the structural analysis of the broader social changes affecting the new economy in which the phenomena of hackers has developed. Cohen's analysis provides a micro-sociological explanation of the processes involved in creating sensationalistic media which will be of use when further attention is paid to media accounts of hacking and how these accounts clash with the hacking community's own understanding of its behaviour. Merton was chosen due to the applicability of his theory in explaining how the actions of social deviants can best be explained by reformulating the research question as the goal or intention of the group rather than simply looking at the activity. The preceding theoretical perspectives will help shed light on the subject of hacking and will be able to answer the various research questions presented at the beginning of the chapter.

Chapter 4 – Methodology

4.1 Introduction

The computer revolution has brought about radical changes in social relationships and has introduced one of the most interesting subcultures – that of the computer hacker. Today, with the advances in technology, those at the centre of the technological culture are creating new communities that exist inside and outside cyberspace. This section presents the methodology that will be used to answer the research questions outlined in Chapter 3.

4.2 Review of Existing Literature

The methodology used to answer the questions outlined included the consultation of books and journal articles. These works were available in various formats. For example, there were hard copies, online copies only or versions available online as well as in printed form. Two types of books were examined, the first being the 'true crime' type and the second being more academic in style. True crime books are generally written by journalists-turned-authors and try to capture the language and the cultural references of hackers, often listing physical descriptions, eating habits and sleep patterns. Although anecdotal, and therefore not empirically valid, these accounts capture some elements that escape more rigid scientific studies. These works tend to feature the case studies of six famous hackers in particular or hacker groups. A key feature of the true crime

books is that they focus entirely on hackers as computer trespassers and not as computer programmers. The importance of these works is that they are examples of the how the media generally treat hackers.

Scholarly books and journal articles are written either by social scientists or by hackers themselves who attempt to provide a more empirical or historical description of hackers and apply an analysis to the phenomenon beyond pop-psychology. The books or articles written by hackers tend to be recognizable by the fact that they are much more technical when presenting a case analysis. Detailing the technological issues of how programs were created demonstrates the author's technological proficiency. An important feature of the selection of hacker writings is that they focus on hackers as both computer trespassers and computer programmers.

Newspaper and magazine articles were also consulted, both online and printed versions. Documentaries, feature length films and television programs were also examined. The importance of these various medias is the way in which the hacker image or myth is portrayed in popular media.

The greatest source of hacker information is on the Internet. Web sites created by hackers for hackers are plentiful. These sites tend to focus on the internal discussion within the computer underground. The material on these sites is sometimes sexually explicit as pirated software sites also contain pirated pornographic

material and cracked passwords to pornography sites. Warez sites often contain links to not only sexually explicit material, but also illegal pornography such as bestiality and rape material.

When travelling on the hacker sites the researcher must exercise caution and travel at their own risk. Anything downloaded, whether it be a file or a program could contain a malicious program which would allow the creator the ability to control the researcher's computer or simply destroy the information. Some sites are also equipped to know who is viewing their site and not let them continue navigating the site.

4.3 New Sources

Other than examining existing print, video and Internet information, the participant observation of a hacker conference was utilized to answer the research questions. The goal of attending the conference was to see firsthand the participants involved in hacking and to examine the way the group interacted. The conference chosen was a semi-annual conference held in New York City called Hackers On Planet Earth (H.O.P.E.). The conference was held in July 2000 and the theme was H2K, a play on the year 2000 computer glitch.

There are other conferences held in the United States such as DefCon in Las Vegas and HOHO in Houston. The decision to attend the New York conference was partially a pragmatic one as HOHO was not occurring that year and H2K was the closest in

proximity and the least expensive. It was also felt that H2K would be the most representative of the hacking environment. The rationale behind this decision was that DefCon is held in Las Vegas, a city with a population of nearly one million, meaning that the vast majority of the 10,000 participants would be from out of town. This in turn could mean that the participants have money to fly to Las Vegas and stay in a hotel. Thus it could be assumed that a large segment would be people who have full-time employment and the disposable income to attend. H2K is held in New York with a population of seventeen million with quick and easy access to surrounding cities. It was assumed that the 3,000 participants of H2K would be comprised of more local people including more youth, more students and those with lower incomes. H2K seemed to be a superior choice due to the vast mix of people from different backgrounds.

The panel discussions attended were on topics that were non-technical and dealt with the media, politics or ethics. The presentations were recorded and shorthand notes were also taken during the events. It was decided beforehand that when interviewing participants, the subjects would be made aware that the researcher was a graduate student writing a thesis on the subject of hackers. As it turns out, dozens of other people were recording the discussions with video cameras or cassette recorders and the need to identify as a researcher never materialized. As a participant observer of the event,

the goal was to note the cultural elements of the interactions between hackers in order to judge the validity of elements generally highlighted by more journalistic descriptions of hacker forums.

In addition to attending the conference, an analysis of hacker emails generated through a list server was possible. A list server is an electronic mailing list where subscribers can post comments for discussion to others who have signed up to the same list and are divided by subject matter. While some are considered permanent lists that span years, others are created for short periods to discuss specific issues. One such list server was created for conference attendants to H2K. This list server allowed for the collection of empirical evidence regarding what interest hackers have and what topics of discussion preoccupy hackers. In a list server the protocol is that one person will send out an email which will have a particular topic to which others will respond, often by pressing the *reply button* in their email software. Usually the original message appears at the bottom of the new message and this is called the discussion thread and allows others to read the original comments that a person is responding to. Included in the emails sent out is the email address of the author which allows the person to be contacted directly for a private discussion. Another particular element of list servers is that the discussions are text based which results in comments that are

usually kept short being little more than four or five lines. Therefore, the general level of debate on the H2K list server was cursory at best.

The original material collected for this research will be used to invalidate the underlying hypothesis of popular media accounts as to the composition of the hacker underground as being made up of nihilistic anarchists. The information will provide for an empirical backdrop from which we will be able to discern what are the principle preoccupations of the underground and interlay these findings with a greater social theory as to the significance of the hacker phenomena.

4.4 Conclusion

The principle methods used to answer the research questions include the examination of hacker writings, reviewing previous works on hackers, participant observation of a hacker conference and an analysis of a hacker list server. This methodology allows for new data to be collected in a scientific manner and for the ability to confirm some of the cultural elements that the journalistic works have highlighted. The next chapter will present the conference and list server results in detail.

Chapter 5 – H2K Conference and List Server

5.1 Introduction

The ultimate fantasy of the digital age – virtual reality – is far from being in existence. Although hackers and science fiction enthusiasts would like to imagine that they live in a digital world, the reality is that humans, and hackers, still live a material existence. As such, hackers have created communities that exist offline that complement those that exist online. In this section these two dimensions will be discussed with an empirical content analysis of the list server that was created for the participants of the conference and a presentation of the participant observation of the H2K hacker conference. Some of the key presentations from the conference that demonstrate the relationship between the hacker community and the information economy will be discussed.

5.2 What is H.O.P.E.?

H.O.P.E. is an acronym for Hackers On Planet Earth and is North America's second largest conference that occurs in New York City. H.O.P.E. is a product of the underground hacker magazine 2600: The Hacker Quarterly[19] that was founded in 1984 by Emmanuel Goldstein. The magazine relies on subscriptions and volunteer articles since it rarely accepts advertising. In 1994, Goldstein and the staff of 2600: The Hacker Quarterly decided to hold a conference in

[19] The name of the journal comes from the frequency that controls the switching apparatus in the telephone networks (2600 hertz).

New York City that resembled the annual conference in Las Vegas entitled DefCon[20]. Although the original conference held in 1994 was hailed a success, the second H.O.P.E. conference entitled Beyond H.O.P.E. was held only in 1997. Entitled H2K, H.O.P.E. 2000 took place on July 14th through 16th. This last conference marks the beginning of a bi-annual event to be held for East coast hackers who cannot attend DefCon, the largest and oldest annual conference.

The conference had no advertisers or corporate sponsors and ran twenty-four hours a day for three straight days. The speakers were offered travel and accommodations in return for their presentations. The registration money was spent on renting the space for the conference which included two stages, lights, video and audio equipment as well as high speed Internet connections so that participants could entertain themselves between presentations. H2K presented itself as an opportunity to observe first hand the various groups of people who attended hacker conferences and judge the validity of media accounts. Due to the fact that the conference operated twenty-four hours with three tracks of speakers occurring simultaneously, not all panel discussions could be attended. The decision to attend one panel over another was based on the topic of discussion. Panels involving ethical, philosophical, political, legal issues or how the media interact with hackers were topics selected.

---

[20] The name comes from the U.S. government's code of military conflict (a rating system ranging between Defcon 1 through 4).

The more technical discussions that focussed on how to produce viruses or how to defeat certain security programs were judged to be of less value given the scope of this study.

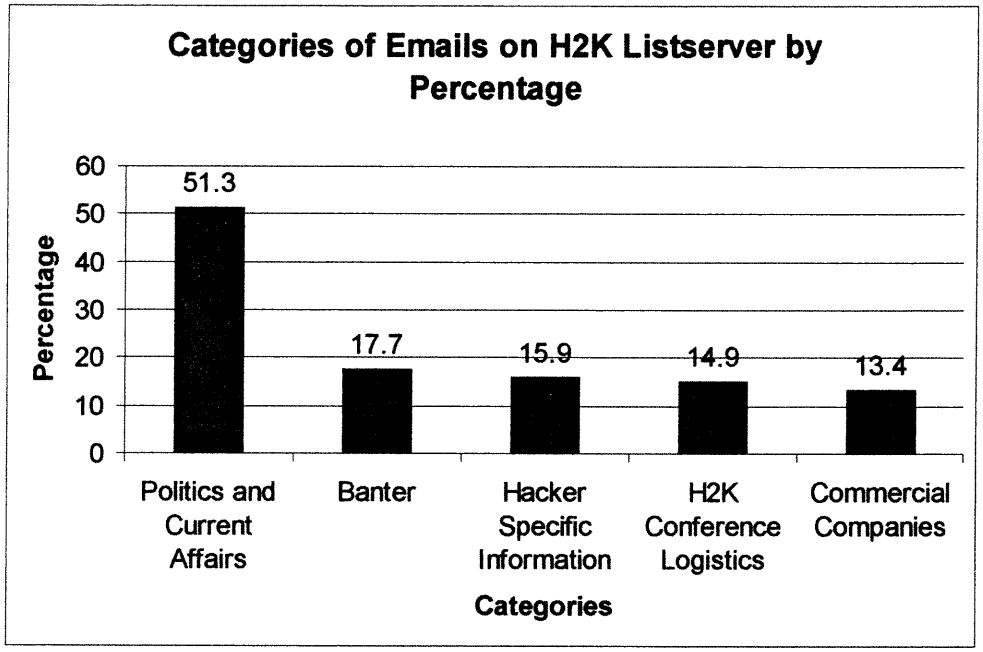
In addition to attending the conference, an analysis of a hacker list server, established for the conference attendants, is included in this study. This presented the opportunity to examine the online interactions between hackers while not interrupting the natural flow of the conversation. Furthermore, the emails received were kept, catalogued and used for analysis in an empirical fashion. Emails were collected from the H2K list server starting in late March 2000, which had already been operating for approximately one month. Every email received for the three and a half months prior to the conference and the six weeks after the conference when the list was shut down was saved. Almost 5,000 emails were received during this period, of which, a random sample of 492 (10%) were kept for analysis. The automated service functions by sending a message to the list server address which is then received by everyone already subscribed. A total of 28 messages contained the commands to *subscribe* or *unsubscribe*. These messages were excluded which left a total of 464 email messages for analysis. The goal was to examine the variety of discussion topics of hackers. One word of caution however: even though topics were discussed, this does not mean that they were

necessarily discussed with great depth or understanding. Many of the emails were curt and consisted of a simple slogan or cliché.

5.3 Online Life: Introduction to the H2K List Server

The following is a content analysis of a random sampling of the emails from the H2K list server. An important element, particular to list servers, is that the discussions are text based which means that comments are often kept short. The postings are therefore generally very short with the majority being little more than four or five lines. As mentioned earlier, the general level of debate on the H2K list server was cursory at best. Most often the issues are dealt within simple clichés or popular catch phrases, although, on rare occasions a long, detailed argument was laid out. The purpose of analyzing the content of the list is to provide a glimpse of what issues are discussed on a list server set up for a hacker conference.

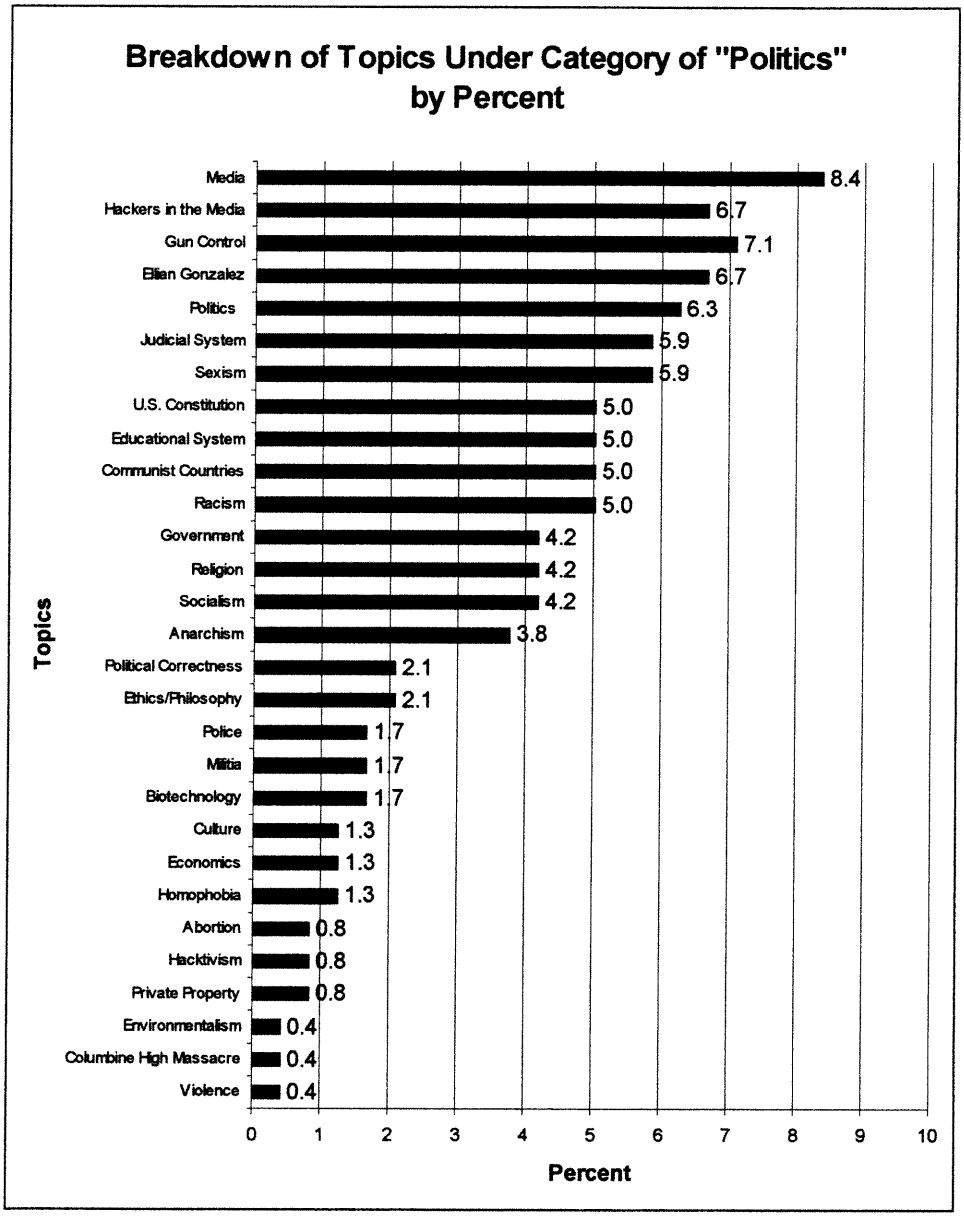
Chart 1 represents the five broad categories that the emails can be divided into.



The five main categories are labelled as 'Politics and Current Affairs' (51.3%), 'Banter' (17.7%), 'Hacker Specific Information' (15.9%), 'H2K Conference Logistics' (14.9%), and 'Commercial Companies' (13.4%). As can be seen in the chart, political issues were the focus of the majority of discussion. The second largest category was labelled 'Banter' for lack of a better term. These postings consisted of personal jokes and quick-witted comments but did not discuss any particular subject matter. The category of 'Hacker Specific Information' contained either technical information, such as programming code, or information as to where an individual could find the answers to their technical questions. (i.e. another hacker's web

site). The category of 'H2K Conference Logistics' consisted of information about the conference, New York, places to stay, what subways to take, as well as plans for socializing at the conference. The final category of 'Commercial Companies' contained information pertaining to commercially available software or hardware including opinions about the usefulness of the products. Emails about technical specifications relating to hacking or cracking commercial software were not included in this category as they were filed in the 'Hacker Specific Information' category. The total of the percentages in the above chart equals more than one hundred due to the fact that the same email could be classified into two or more categories at once.

Chart 2 gives a complete breakdown of the topics that were broadly classified as 'Politics and Current Affairs'.



Under the broad category of 'Politics and Current Affairs' a total of 29 distinct topics can be found. The largest amount of emails

dealt with the topic of media (8.4%) and hackers in the media (6.7%). I made the distinction between media and hackers in the media because there was clearly a subset of the media category where participants discussed media reports about hackers. Within the category of 'Media' we can find a variety subjects that revolve around the corporate control of the media and the types of articles presented in relation to other current affairs discussed in the mainstream media (such as the Ellian Gonzalez affair, the demonstrations at the Democratic and Republican conventions). Hackers seemed to be very interested in talking about how they are perceived in the media and what are the types of things that are being said about them. Many of the postings in this sample were individuals that simply gave the Internet link to where a current news article about hackers was or copied and posted the entire article for everyone to see.

The next two most debated topics were gun control (7.1%) and the Ellian Gonzalez affair (6.7%).[21] The gun control debate is one that is almost unique to the United States where opponents are very vocal and the debate often leads to a discussion about the U.S. Constitution (5.0%). In the Ellian Gonzalez debate many other topics flowed from it such as the situation in Cuba or other communist

[21] Ellian Gonzalez was a 5 year old Cuban boy who's mother died on their sea voyage to the United States. There was a lot of media attention and pressure put on the U.S. government to either return the boy to his father in Cuba or give him to relatives in Miami.

countries (5.0%), socialism (4.2%), anarchism (3.8%) and the role of the government (4.2%).

Politics (6.3%), the judicial system (5.0%) and sexism (5.0%) were also highly debated topics. Under the category of politics one could find comments on the Democratic and Republican conventions, the way public decisions are made in democracies and the relationship between citizens and their representatives. Broadly categorized as the 'Judicial System', emails about hacker trials, the legalities of retrieving items from dumpsters and information about legislation belonged to this category. The topic of sexism was often discussed in conjunction with homophobia (1.3%), abortion (0.8%), political correctness (2.1%) and racism (5.0%).

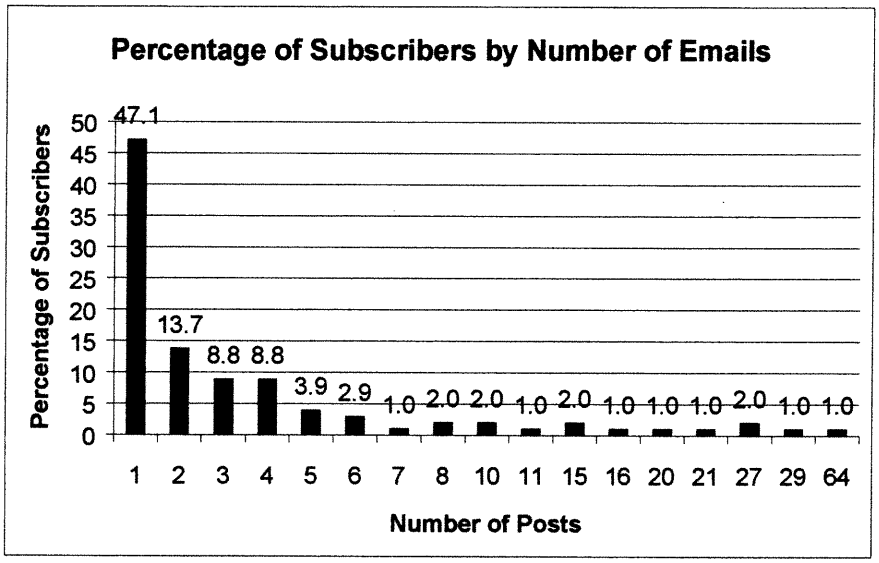
The educational system (5.0%) was discussed in relation to its limitations and the influence of religion (4.2%) in the public school system. Other topics discussed on a more infrequent basis included; ethics/philosophy (2.1%), police (1.7%), militias (1.7%), biotechnology (1.7%), culture (1.3%), economics (1.3%), hacktivism (0.8%), private property (0.8%), environmentalism (0.4%), the Columbine High massacre (0.4%) and violence (0.4%).

A further analysis of the "Politics" category illustrated some interesting elements of the hacker underground. It is not possible to make a blanket statement about the views espoused by hackers when discussing political or philosophical topics. For example, debate

surrounding the Elian Gonzalez affair often featured a discussion of parental rights and would eventually lead to an attack on Cuba, Vietnam, the Soviet Union and communism in general. Following the same 'right wing' viewpoint, there was a tendency to attack feminism and "political correctness" (although what that meant was never clearly defined). Although there were some supporters of the right to fly the Confederate flag, most argued that it was a symbol of a racist era. The only two issues where there was unanimous agreement was in support of freedom of speech and of the belief that the mainstream media consistently paints the incorrect picture of what hacking is all about.

Another key point of interest in the examination of the list server postings is how many of the emails were sent out by the same person. For example, the majority of list server members only posted one email (47.1%). Chart 3 provides a breakdown of the number of postings made and the proportion of people that made that number of postings.

Chart 3



Those who posted five or more emails account for over one sixth of the cases (21.8%). A relatively small number of participants were able to dominate the discussion as the top three participants accounted for one quarter of the total postings (120 out of the 464 total).

One of the possible difficulties in using a sample of this nature is in the ability of those responding most frequently to skew the results. For example, in this sample if the top three respondents had chosen to discuss only the media then this would give a distorted view of what issues were discussed by all respondents. Fortunately, the three dominant respondents in this sample discussed a variety of issues in addition to responding to the questions and comments posed by other hackers.

5.4 Description of H2K Participants

Based on media reports of who hackers are, one would expect a hacker conference to be filled with young teenage boys, socially awkward with unusual hair cuts and glazed over eyes due to an infinite amount of time staring at computer screens. In other words, the stereotypical computer geek.[22] Although it is true that a vastly disproportionate amount of men attended the conference, the variation in age was quite apparent.[23] Levy's different generations of hackers were present at the conference as was demonstrated with the older participants telling tales of early hacking exploits to eager newcomers to the subculture[24]. Far from being monolithic in dress code, some of the attendants wore suits while others were dressed in punk rock and

---

[22] A typical statement about hackers includes "Could it be that our nation's young computer brainiacs have decided to spend less time hacking and more time chasing sports or the opposite sex?" (Hogan 2000*). The image created by this type of comment is that of an individual who lacks physical coordination, is shy and has an inability to attract a mate.

[23] Only two of the panellists were women from the presentations attended by the researcher, and both of them were non-hackers (one was a lawyer from the Electronic Frontier Foundation and the second was a researcher from Laurentien University).

[24] Captain Crunch, an infamous phone phreaker, named that because he discovered the sound from whistles given out with boxes of Captain Crunch cereal in the 1970's could reproduce the frequency needed to control the telephone networks. As an icon of the phreaking and hacking underground, he was more than happy to tell stories from yesteryear dressed in a tye died shirt with disheveled gray hair.

industrial fashion.[25]

There was a great variation in age and in dress at the conference. When discussing technological issues people from different generations and social classes interacted with ease. The unifying issue of hacking seemed to erase the classic hierarchy of age within the group. One panellist who was no more than twelve years old appeared on the Retro-computing panel with two other computer enthusiasts in their fifties[26]. Although the young panellist had not lived through the early days of personal computers, he was an avid collector and was accepted by the group to speak authoritatively on

---

[25] The issue of counterculture and music and its relationship to hacking is very interesting. In North America the counter-cultural youth subcultures started with the Hippy movement in the 1960's and 1970's. Although disco was an important influence in the 1970's, it was more cultural than counter- cultural. The next counter-cultural movement was the Punk Rock movement in the late 1970's and early 1980's. One key difference between the Punks and the hippies was that the Punks were much more aggressive and violent towards each other and towards the symbols of the State. This difference was exemplified by the fast pace of the Punk music and in the style of dress which included leather jackets with metal studs, spiked hair, and steal-toed boots. Both the Hippy and the Punk counterculture have in common the ludite spirit. The musical instruments used by both were the same.

The next popular youth cultural movement that occurred during the declining phase of Punk in the early 1980's was New Wave. The introduction of synthesizers and drum machines made New Wave music break with conventional music and the Punk and Hippy past. Although New Wave was still a mainstream youth culture, it gave the fertile ground for the Industrial underground to grow. Hippies and Punks can be said to be counter-cultural because they include social and political projects as well as a musical and fashion scene. New Wave and Industrial do not have the subversive political movement associated with it. The Industrial subculture can be described as the fetishization of technology. Where as New Wave was replacing manual instruments with technological imitations, Industrialists saw technology in music as the end rather than a tool. Industrial music is characterized as having a dark technological element. Clothing is usually the black leather jacket and steel-toed boots just as the Punk, but without the political slogans and the spiky hair. The Punk style of dancing is a mosh pit where individuals jump and bump into each other; therefore there is a necessity of having many other individuals to dance, whereas the Industrial method of dancing is individualistic, swaying the body without touching another individual. The current most popular youth subcultures demonstrated by hackers at the conference was a mix of Punk and Industrial.

[26] "RetroComputing" (Graphix, Mr. Ohm, Nightstalker, and Sam Nitzberg 2000).

the subject. The majority of panellists observed were white men who were in the work force and a smaller number of young hackers who were too young to be fulltime workers. There was a much greater ethnic and gender diversity amongst the attendees and volunteers of the conference than the presenters.

5.5 Analysis of topics of discussion

Below is a list of all of the scheduled panel discussions at H2K. The researcher attended those that are in bold.

1- **Why Hacking NASA is a Stupid Idea**
2- **Selling Out: The Pros and Cons of Working for the Man**
3- Secrets of the DNC/RNC (H.O.P.E. was taking place before the Democratic and Republican National Conferences. This panel discussion was about how the Secret Service was going to protect the events and included a list of radio frequencies which the Secret Service, the FBI and the local police use to communicate so that any one could join in and listen to what was being said over the airwaves.)
4- **Ethics in Military and Civilian Software Development**
5- GSM and CDMA (The panel discussed the next generation of mobile phone technology.)
6- **High School Horror Tales** (A panel of hackers in high school tell stories of the trouble they got into because of their knowledge of computers.)
7- **Counterfeiting IDs and Identity Theft (This was more of workshop than a panel discussion.)**
8- Hacking Consciousness: Back cover Text (Chris McKinstry attempts to make the case that consciousness and meaning evolved to help us survive in a socially complex world, and that the same process can be duplicated inside a computer.)
9- **Hactivism - Terrorism or a New H.O.P.E.**
10- **The Legal Panel** (What is legal and illegal in computer hacking and what laws are coming into effect.)
11- Internet Security Using Open Source Software
12- **Cyber Civil Disobedience**
13- **Becoming the Media - How the Web is Changing Everything** (A discussion about alternatives to mainstream information agencies.)

14- Cracking the Hacker Myth: A Scientific Study to Find the Real Story (A Laurentian University Hacker Research Team has been undertaking an independent study to create a balanced view of hackers.)
15- "Freedom Downtime" (The premier of a documentary made by Emmanuel Goldstein about hackers.)
16- Security Through Gaming: The Cyberwar Game (This workshop was a night of computer gaming with teams divided up.)
17- Low Power FM (LPFM) (This discussion was about establishing a pirate radio station.)
18- **The Old Timer Panel** (Hackers who have been around since the creation of computers discuss old systems and old hacks.)
19- Low Bandwidth Access to the Internet (Bringing the Internet back to its roots, text based access to information.)
20- Retro Computing (Old computers are discussed such as the TRS-80 and the Atari 800.)
21- **How I Got My Own Area Code** (Known as one of the greatest hacks of all time, the Cheshire Catalyst explains how he got his own area code (321) in Florida.)
22- The Hacker's Code (Ethics in hacking)
23- The King's Mob Open Source Mediamaking Panel (A local media do-it-yourself group describes how to create alternative media outlets.)
24- The Robotic Graffiti Writer (A robotics collective shows off their latest invention, a remote controlled graffiti machine.)
25- Ethics in the Hacker/Phreaker Community
26- **Cult of the Dead Cow Extravaganza** (An elite hacker group put on a light and music show.)
27- Shortwave Radio - Precursor to the Net
28- Hardware & Electronics Q&A Panel
29- Hackers and the Media (A panel of journalists explain why hackers get the press coverage that they do.)
30- Napster: A New Beginning or Beginning of the End? (A computer site which allows people to post all of their CDs and download any song in stock for free.)
31- Nootropics (Nootropics are chemicals that enhance one's abilities such as memory retention and thought creation. A discussion about these products, legalities and where to obtain them.)
32- **Mock Trial - The MPAA vs. 2600** (The Motion Pictures Association of America is suing *2600* and Emmanuel Goldstein.)
33- Spy Stuff: Everything You Never Believed But Wanted to Ask About...
34- Bypassing Modern IDS Products (A technical workshop.)
35- The Internet - The View From Overseas
36- Being a Good Samaritan Online

37- Telephone Systems of the World
38- Information on the Masses (A private investigator details all the information anyone can access about anyone else completely legally in the United States.)
39- Introduction to Computer Viruses
40- Parents: Are They Your Enemies? (A panel of parents discuss how they try to give guidance and set examples for the younger hackers.)
41- Pirate Radio 101
42- The Jon Johansen Story (A young Norwegian hacker is being sued by the MPAA for writing some computer code.)
43- The Web is a Harsh Mistress (What keeps systems secure?)
44- Number System Conversion (A calculus course for hackers.)
45- Social Engineering Panel (A discussion about how to talk your way into any event and get any information.)
46- Internet Radio
47- Lockpicking
48- Hackers Of Planet Earth (Discussion with hackers from other countries.)
49- **Has Anyone Learned Anything?** (A discussion about corporations and governments and what have they learned about computers.)
50- **Keynote Speaker Jello Biafra** (An icon of the 1980's North American punk rock movement, he was the lead singer for the Dead Kennedys.)

Some of the presentations did not occur because the schedules did not permit them or there were difficulties with the arrival of the panellists. Twenty-seven (54%) of the presentations focused on what can be broadly categorized as the social relationships of hacking while twenty-three (46%) focused on specific technical issues. This means that roughly half of the presentations discussed political, social, legal issues or how the media and other outsiders treat hackers. This demonstrates a high level of self-awareness regarding how hacking is a deviant activity and how there are specific issues that must be thought about when one enters the world of the computer

underground. Presentations such as "Why Hacking NASA is Stupid" and "Selling Out: The Pros and Cons of Working for the Man" represent a conscious effort to socialize future hackers and newcomers to the subculture. This also demonstrates that there is self-awareness that hacking is something of a philosophical pursuit as well as technical.

The other half of the presentation topics that dealt with technical issues demonstrate the high level of dissemination of knowledge between the participants. Panel discussions such as "Counterfeiting IDs and Identity Theft" and "Introduction to Computer Viruses" were more like workshops than traditional panel discussions. There was a high level of interaction between presenters and audience members in an open atmosphere of teaching. Throughout the three days many elite hackers could be found in the hallways surrounded by less technologically proficient hackers eagerly listening to every word spoken about a particular system or method of programming. The majority of people were eager to discuss specific technological issues and to brainstorm about ways of circumventing existing barriers. Before ending their presentations, panellists announced what room they would be in after the event in order to continue discussing issues and answering questions.

5.6 Ethical Self-Consciousness

Far from being a group of nihilists determined to destroy society's information infrastructure, hackers at this conference seemed keenly aware of the philosophical questions surrounding their activities. For example, four panel discussions at H2K were organized that focused specifically on the ethical considerations of hacking, and are discussed in detail in the following paragraphs.

In Chapter 2 of this paper Newby's "Hacker's Code" was presented as one of the most recent articulations of the hacker's ethic. Newby presented a draft of his code at H2K and made his presentation an interactive discussion in order to solicit opinions from the group on the subject ("The Hacker's Code: H2K". Newby 2000). The importance of his presentation was not necessarily the actual discussion or code that developed, but rather the fact that the topic was an interest and concern to some hackers. This demonstrates awareness on the part of hackers that there is a need to set boundaries to their activities. Newby's presentation can be seen as a form of community self-regulation and an important part of the socialization process for new hacker members. It also represents an attempt for the community to define themselves. This code of ethics was created for the purposes of articulating what a 'real' hacker is supposed to be.

Nitzberg, Shwartau and Steele, other panelists at H2K, chose to focus on the programming element in their panel discussion entitled "Ethics in Military and Civilian Software Development" (Nitzber, Shwartau and Steele 2000). The main message that these panellists conveyed was that there should not be a difference in the way a person approaches programming military software to programming commercial software. Generally speaking, there is a perception that when programming military applications a greater level of care should be exercised as lives are often dependent on software that functions properly. Commercial applications, it reasons, can be a little more lax due to the fact that the programs are not life threatening. Steele made the argument that commercial software is just as vital as military, if not more so, due to its application in many industries that society depends on and could have catastrophic effects should a problem with a program arise.

While Microsoft was considered as the chief enemy of productivity due to errors that often appear when being used, the focus of hostility at H2K were all programs that contain bugs. When a program shuts down or does not do what it is supposed to it slows down productivity and people's time is wasted. A highlight during the discussion was the fact that in the United States a license was needed to cut people's hair but a license or accreditation is not needed to write a program. This is an example of people demanding higher standards

and a desire for more stringent accreditations to becoming a programmer.

During the "Being a Good Samaritan Online" presentation, Wignall argued that when traveling the Internet most hackers come across sites with security holes (Wignall 2000). He questioned the audience about what should be done in these circumstances. Should a person; A) hack it/deface it/rob it, B) ignore it, or C) report it? He assumed that an ethical person would report it. However, is it possible to report the hole given certain circumstances? A person must make sure that the way the hole was found was not through illegal means in their country, in the company's home country and in the web hosting company's country. If legitimate, who does one report it to? A person could tell the web hosting company, but, according to Wignall's experience they rarely fix a security hole reported by an outside source. The media is not interested in a security hole unless the site has been hacked. The Webmaster at the company who is in charge of maintaining the site has an interest in not letting his/her supervisors know about their incompetence. A sales person for the company is often not interested. The public relations or marketing section might be interested because they fear bad publicity. Management may have an interest or they could be inclined to call the police. A member of the audience proposed contacting the clients of a company, such as the shoppers purchasing online products from the company in

question. Wignall proposed one last alternative which is something he is building specifically for reporting security holes. This alternative is a third party info-warfare hotline in which a reputable government or non-government organization is contacted by a hacker. The hacker's anonymity would be guaranteed by law and the company who's security had been breached would be notified of the hole.

Until an organization like Wignall's third party hotline is created and protected by law, the most effective method is contacting the senior management of the company by letter. Furthermore, he says that a person should not expect a thank you letter or even a response. In fact, if a name is given, the company may trace the letter and the police will be informed and legal action may be threatened by the company's attorneys. The presentation highlighted the fragile relationship that helpful hackers have with the current system of law.

The final panel discussion dealing with ethics was "Hactivism – Terrorism or a New Hope" (Shapshifter, Bronc Master and Oxblood Riffin 2000). The panel consisted of two hackers who are members of Cult of the Dead Cow (CDC), an elite hacker group, as well as an activist who assisted with the organization of the WTO demonstrations in Seattle and the IMF demonstrations in Washington. Although it is generally understood that hacktivism is the melding of activism and hacking, there is no formal definition. Bronc Master, one of the presenters, stated that a question that should be asked of hacktivists

is: "Did you pick your cause before you picked your site, or did you pick your site and then pick your cause?" (Bronc Master 2000). If a person defaces a site and then justifies it because the corporation or the government had done something they disproved of, this is simply vandalism and should not be labelled hacktivism. If, on the other hand, a person objects to a group and they attack their site because of this objection then this qualifies as hacktivism. The motivation behind the action needs to be questioned in order to distinguish between hacktivism and vandalism.

The activist on this panel, Shapeshifter, participated in the conference to encourage hackers and activists to work together for the sake of progressive politics. He believed that hackers and progressive activists have common issues and beliefs that complement each other. Oxblood, one of the CDC hackers, was much more conservative regarding his notion of hacktivism. For example, the CDC does not support Shapeshifter in attacking Nike's web site because by the same logic someone who disagreed with his message would be able to attack Shapeshifter's site. Thus, this type of hacktivism is narrowly focussed on destroying people's sites. Oxblood believes in open access to the Internet and in destroying barriers to open access. He and a group of other hackers are currently involved in a project to destroy the Internet firewalls of China, Cuba and North

Korea[27]. According to Oxblood, the only activism hackers should be involved in is the facilitation of freedom of speech and freedom of access to alternative information.

The central issue of contention for the panellists was how to justify malicious hacking. The question lies in what constitutes an appropriate target and the length a person should go. Some panellists drew the line at defacing web sites while others argued that computer viruses are acceptable. A major difficulty with a hacktivist is in making the public aware that a hack was done for purely political reasons rather than an opportunistic attack.

These four presentations demonstrate the debate occurring in the hacker community regarding their ethical conduct. This shows a consciousness about the effects their actions have on society and an awareness about how they are viewed by non-hackers. These presentations also provided a socialization process for new hacker in attendance.

5.7 Conclusion

The most interesting and significant element to the H2K conference is its very existence. The fact that the hacker phenomenon has become so pervasive that there can be a three-day conference in which people from across North America come to

[27] A firewall is a security program that determines which sites a person may visit. By disabling a firewall the person would have the ability to view every site on the Internet.

discuss topics of this nature speaks to the growth of hacking and the meaning that participants draw from it. The variety of topics discussed ranged from politics and ethics to the minutia of computer programming which reflects a community that has more than computers binding them together. There is a complexity in the nature in which they relate to one another.

The fact that the conference was open to anyone who paid the forty dollars entrance fee speaks volumes as well. A far cry from the cloak and dagger image of computer hackers and the security agents that follow them through the maze of the Internet, this was an open event where one could proudly walk among fellow hackers. Those that gave workshops on virus writing and technical information about the circumvention of various programs stated that the knowledge was intended for academic purposes and not to be applied in real life. However, the verbal disclaimers spoken through grinning faces could not be taken seriously, as there was a tacit understanding that many of tips learned would be applied shortly after the conference.

There is a degree of arrogance in the way that hackers disseminate delicate technical information. At the back of 2600: The Hacker Quarterly, a listing of monthly hacker meetings in various cities around the world can be found. All of the meetings take place in the lobby of a large corporation or a coffeehouse where anyone can

identify the participants or listen in on the discussion. This openness reflects the strong philosophical belief that hackers have, which is what they are doing is neither wrong nor immoral. The actions that are considered illegal are thought to be illegitimate criminal offenses and reflect an overbearing State that is acquiescent to the lobbying of corporations.

Far from being a monolithic subculture creating like-minded individuals, a certain level of political autonomy still remains. Hackers come from different backgrounds, nationalities and social and economic classes. There is a wide range of beliefs on political and social issues. As a generalization, the sole area where hackers have similar beliefs is in regards to freedom of speech and the right to ask questions. A curious mind is the hacker's best asset. Furthermore, hackers share certain cultural traits. Although many youth subcultures are present within the computer underground, a common reference point is science fiction movies and books. There is also the development of a specific language to the subculture. This element becomes very apparent when analyzing online works. Hackers write in a phonetic manner, often substituting proper spelling for truncated words or expressions. Although orally hackers have a distinct vocabulary, the wording found online is probably more a reflection of the text-based communication rather than the development of new words for the subculture.

There is undoubtedly a high degree of knowledge transmission during the conference, witnessed either formally during panel discussion/workshops or informally in the halls of the hotel. Some have interpreted the willingness of hackers to discuss their exploits as nothing more than insecure people trying to gain a reputation for themselves. Could it really be that three thousand egomaniacs spent three days and nights trying to out-do their counterparts in a bid to look the 'coolest'? This explanation is too simplistic. The answer to this question lies in an understanding of the hacker ethic and how it relates to a movement that is trying to legitimize its knowledge base and trying to change the way people think about technology.

Chapter 6 – A Reflection on Hacking

6.1 Introduction

In this final section the key question that has motivated this study will be addressed, namely, how is the hacker movement to be interpreted? The newness of the phenomena of hacking and the issues surrounding the phenomena present difficulties in providing a coherent and structured analysis. In order to accomplish this daunting task, the new paradigm of the information economy iterated by Bell, Touraine and Castells is used to examine the role of hackers as powerbrokers in the information society and in considering how their power is exerted. The two principle ways in which hacker power is exercised is through the hacker method of software production as well as through the circumvention techniques that are developed and shared with the public. These manifestations of hacker power have become the focus of public scrutiny through the eyes of the media. The relationship between the media and hackers will be examined in the following paragraphs, as well as the paradoxical image of the phenomena that has developed. In this image hackers are portrayed as nothing more than nuisances or as the next ungodly plague bent on destroying civilization. Although media hysteria surrounds hackers, they are still being integrated into the mainstream economy willingly. How is it that hackers would be willing to become a cog in the great corporate machinery and why would they be willing to describe their

exploits to the world including technical details? Through the application of Merton's theory of cultural adaptation it will be shown that hackers can be interpreted as a rebellious group determined to change the relations between producers and consumers of programmable technologies reflecting a democratic movement challenging current power structures.

6.2 Hacker Influence

Although information technologies have not reshaped society as fundamentally as futurists had forecasted, there are new groups that have developed. As was demonstrated earlier in Chapter 2, the information economy has brought with it a new class of people, namely, those that can control the spread of new communications technologies. Hackers are part of this group and their power grows with the diffusion of programmable technologies. They exert their influence by being at the forefront of technological developments, as well as through the circumvention of security barriers.

Hackers have heavily influenced the development of the Internet, the most important communications tool recently developed, demonstrating that they are at the centre of innovation[28]. The recent example of Napster illustrates how one individual can change the way

[28] It is with the involvement of hackers with the creation of bulletin boards and the development of online communities that enticed more and more people into the digital realm.

an entire industry distributes its commodity[29]. These examples show the effect hackers have on the way the rest of society communicate and consume products and services. Companies and governments are openly recruiting computer hackers due to the high level of competition they face with high-tech firms (Hulme and Kontzer 2000*, Glasner 1999*). Just as the record music industry sends talent scouts to the marginal elements of the counterculture, so do the entrepreneurs of the highly volatile high-tech sector. Although hackers do not occupy an official place within the corporate hierarchy and are not recognized as powerbrokers of the information age, they do in fact exert influence over the new economy by being at the centre of innovation and of computing trends.

Hackers also exert their power over the information economy by circumventing technological barriers. By highlighting the lack of security on the Internet hackers raise the awareness of consumers to the dangers of purchasing products online and having their private information flow through networks. E-commerce is still in its infancy partially due to a public perception that travelling online presents the risk of having nefarious members of the computer intelligentsia steal their credit card numbers or steal their entire identity (Niehaus 1998*).

---

[29] Napster is a music file swapping program that allows users to download music for free from the Internet. The program was written by a college student in an evening. The author of the program was sued by the major record labels in the United States and eventually signed an agreement with them to shut down his free site and start a pay-per-use site in conjunction with the recording industry (Mann 2000: 40).

Whether this fear is real or simply a perceived threat, consumers are only slowly adopting the new consumption habits of the twenty-first century. Emails can be read, credit information can be unearthed, services can be easily interrupted in the digital age. Those who are agile enough to find their way through the electronic maze can exercise power over others in an unprecedented way. Previously, a person had to cut a telephone line to disconnect service, whereas now, a person can change the billing information from across the planet, completely mobile with a laptop and a cell phone. In the case of politically motivated hackers, a government or corporation could easily find itself under siege electronically with production disruptions due to one unarmed person[30]. In a hyper-individualistic world, the new information age provides the tools for new unprecedented powers to be exerted by a specific type of individual – the computer hacker.

The examples above highlight how hackers influence the market place illustrating their importance in the information economy. The issue of power is an important step in understanding how hackers relate to the larger society in the digital culture of the new millennium. Because of this dual role of innovator and saboteur, hackers have

---

[30] The ElectroHippies are an example of the use of the Internet for political purposes. They state "the main aim of *the collective* is to develop a debate about the use of the Internet for campaigning, and also the notion of the Internet being the largest of all the *'global commons'* — the concept that the nature of the Internet makes its use open to all, and that areas of the Internet should not be arbitrarily annexed or controlled as has happened to large areas of the real world during the last four centuries" (The Electrohippies Collective 2001*). They have organized electronic demonstrations that have shut down web sites of governments and multinational corporations.

gained a reputation with the public that oscillates between Dr. Jekyll and Mr. Hyde.

6.3 The Relationship Between Hackers and the Media

The media is not a monolithic entity with a common party line, toed by corporate bureaucrats throughout the 'free world'. Nor is the media an objective distributor of information, free of biases, whose goal is to inform the citizenry enabling them to make sober discisions about the world around them. After reviewing the picture of the hacker as painted by the media and comparing it to what hackers themselves say they are, one of the key questions is why is the public's definition of hacking so different than that of hackers? As was demonstrated in Chapter 5 through an examination of the topics raised at the hacker conference as well as the issues discussed on the list server, hackers spend a great deal of time discussing the way the media portrays them. As a marginalized group in society, hackers have a cantankerous relationshionship with the media. Two themes emerge when reviewing news accounts of hackers. The first is that the discourse surrounding hacking usually stresses the financial ramifications and economic disruption[31] that is created by the activity and the second is the stereotype[32] of the hacker as presented by the

---

[31] Examples of this include, "Hackers cost firms billions of dollars" (Geralds 2001*) and "Hackers Said To Cost U.S. Billions" (DeLong 2001*).

[32] Platt describes the participants of the first H.O.P.E. as "A mob of scruffy, geeky guys.." (Platt 1994*), while Evanson and Quinn describe one of the most infamous hacker as "...a picture of a lonely, social misfit..." (Evenson and Quinn 1995*).

media. The relationship between hackers and the media is governed by a macro process in which financially dependent media producers rely on advertisers as well as a micro process where the need to attract consumers leads to the creation of tantalizing stories. These processes, discussed in more detail below, work as a whole to explain why the media presents the image of the hacker and frames the debate as it does.

Many authors have detailed the variety of structural influences that determine what is presented in the media and how it is presented (Chomsky 1989, Herman and Chomsky 1988). The overall framework in which the media operate in the free market is that media outlets make a profit by delivering consumers to advertisers (Chomsky 1989: 21). The bulk of the revenue is made by advertisements and this dependency of the media on advertisers forces the tailoring of news to the wishes of advertisers (Chomsky 1989: 23). If a news agency consistently produces stories that go against the interest of the advertiser, it is only logical that they take their advertisement dollars else where. In the overall framework of corporate media certain truisms are consistently presented. The legitimacy of the relationship between owner and worker is continually reinforced, the dominance of a profit mentality never falters and the underlying assumption that self-interest is the motivating factor in human action is static. Therefore,

given the structural limitations of corporate, for-profit media, it is understandable that when hackers are discussed in the corporate media the story is virtually always framed as a profit issue. How much money did the hacker 'cost' the company? For example, what was the lost revenue from services used for free, lost revenue from paying customers who could not purchase items, lost future customers due to negative media surrounding the hack attack. These are the types of questions that are repetitively presented in the media when discussing hackers. This macro analysis by Chomsky about the structure of media production in the free market helps understand some of the larger elements framing the presentation of hackers to the public.

Simultaneously, a micro process is at work. This is the need to create sensationalistic stories in order to attract consumers. The concept of a moral panic by Cohen helps explain the flood of articles about hackers (Cohen 1980). Hackers are presented as a group determined to destroy civilization with a lack of respect for personal privacy and property. The distorted and exaggerated picture that the media presents is the central criticism that the hacker community levels at the mainstream press. Hacking is presented solely as a criminal pursuit, as a game of cat and mouse in which youthful computer enthusiasts break-in to snoop around networks and destroy or vandalize data. Under the banner of cyber-terrorism, countless

news articles and experts declare that computer disturbances lead by hackers will be the new face of the apocalypse[33]. On rare occasions, the media prints false stories that appear credible to the editors of the news agency because it simply reaffirms the stereotype[34]. Predictions are used by the media to stir up a moral panic[35] and the use of dramatized and ritualistic interviews with representative members of the computer underground help reaffirm the stereotypical vision of the hacker[36] (Cohen 1980; 42). Chomsky and Cohen provide the macro and micro theoretical framework for understanding the relationship that the media has with hackers and why the media consistently presents a definition of hacking that is different than the one hackers have.

Given these differences, one should question why hackers bother interacting with the media. If the media rarely presents hackers in a positive light and the picture is always distorted, then it seems odd

---

[33] Articles such as ABC News' "Computer experts are warning cyber-terrorism could strike the Sydney Games" (Sales 2000*), CNN's "Feds take steps against threat of cyber terrorism" (Wasserman 1998*), MSNBC's "Pentagon and Hackers in 'Cyberwar'" (Miklaszewski and Windrem 1999*), and the Globe and Mail's "Canada called 'hacker heaven' for criminals" (Ross 1999*) all give the impression that the world is being held hostage by computer hackers. With statements like, "Justin Davis, a 20-year-old convicted computer hacker from Thunder Bay, says he hasn't met a system yet that he couldn't break into," (Ross 1999*) readers get a sense that nothing is safe.

[34] Such as the Glass article "Hacker Heaven" that appeared in the *New Republic* and was eventually admited to be completely a work of fiction (Penenberg 1998*; Goldstein 1998).

[35] Articles such as, "Hacker attacks expected over New Year's weekend" (Reuters 2000*), and "Copycat hacker attacks expected now, experts predict" (Rose 2001*) all give the sense that waiting just around the corner is a new round of attacks that will cripple communications technologies of major corporations.

[36] As demonstrated in the Zone Libre (1999) and MTV: True Life (1999).

that elite hackers such as Oxblood Ruffin, Kevin Poulsen and Emmanuel Goldstein would bother giving interviews. The reason, according to popular psychology is that hackers are motivated by an insatiable appetite for bragging about their exploits[37]. They want to be recognized as cool, powerful or important people in the world. This explanation is too simplistic and might apply to the young teenager in high school, but does not hold up for the older hacker who is a professional. I believe that this willingness to interact with the media represents an underlying movement within the computer underground to change the way society views technology and the transfer of knowledge. In order to accomplish this goal they must challenge the false image created by sensationalistic corporate media. If hackers wanted to be feared or admired because of their exploits, one could reason that they would not be interested in telling the technical details of how they broke into a system. Rather, they would be more interested in keeping secrets in order to create an air of mystery and give the impression that they are special and highly talented. The reality is that hackers spend their time explaining in great detail exactly how anyone can do what they did. Far from increasing power and prestige, this willingness to teach others simple computer maneuvers

---

[37] Here is a typical statement; "Fighting hackers is like fighting graffiti... Their biggest kick is to damage a system and then brag to all their friends. If you get rid of the damage, there's nothing for them to show" (said by a security specialist as quoted by Appleyard 1997*).

actually takes away from their uniqueness and mystery. Therefore, the question remains: why do hackers share their knowledge particularly regarding the media?

If explaining how they completed their exploit takes away their power, then why then do hackers tell the world? Returning to the hacker ethic illustrated in Chapter 2, hacking is about pro-active learning and discovering new and inventive ways of using things. It is about sharing information and learning from others in an open atmosphere which leads to innovation. The motivation for telling all of their secrets is that hackers want more hackers. They want everyone to think of themselves as hackers and to rediscover the curiosity that is innate in human beings. Furthermore, by demystifying hacking and computers, hackers are helping to insulate themselves from the criminalization process that is currently underway. By demonstrating that hacking is not harmful and that the same rules that govern material possessions cannot be applied to computer technology, hackers help educate the public and lawmakers in understanding that new solutions to new issues need to be developed. Currently there is a vacuum of technologically proficient people in power, whether it be in parliament or in the judiciary and as such, activities which resemble trespassing are being treated as terrorism.

6.4 Hacktivism

The analogy of hacking as terrorism leads to the political question of hacktivism. Far from being a homogenous group of people, hackers represent a broad spectrum of political beliefs. As was demonstrated by the analysis of the discussions that took place on the list server, hackers range from free market enthusiast to staunch supporters of State intervention in the distribution of resources. Regarding social issues, hackers also demonstrate a wide variety of opinions from those who hold mildly sexist views to radical feminists and militant gay rights activists. What binds hackers together is the belief in the freedom of information and an obsession with technology.

This lack of homogeneity leads to a deep divide within the hacker community regarding the use of hacking as a legitimate political tool of dissent. Proponents of hacktivism argue that civil disobedience has a long tradition and is a legitimate form of protest and applying the hacker methods to political activity is a natural progression as society becomes more dependent on technology. This allows a redefining of the power relationship, where one individual can now halt production. Detractors of hacktivism argue that political involvement is cliché and serves as nothing more than a justification for people to indulge in nefarious hacking activities. Furthermore, hacking is about the free flow of information and critics of hacktivism

argue that a single person does not have the right to silence another online (which is what happens when a web site is shut down temporarily). What this conflict demonstrates is that at the heart of hacking is an underlying liberal democratic viewpoint. The reason why even anti-hacktivism hackers such as Oxblood Ruffin would attack Chinese and North Korean firewalls and not the web sites of the non-communist governments with an equally poor reputation for civil liberties, is because of the belief that if information is freely exchanged then human rights oppression and other forms of oppression will eventually disappear. If people can speak freely and have the same civil liberties as Western democracies, then they can free themselves from oppression. The fact that the major problem of most third world countries is that income distribution is completely distorted leading to a lack of basic necessities such as food, potable water and medical supplies, does not enter the discourse of the hacker. Material conditions are irrelevant as political thought and economic systems seem to flow from the free exchange of ideals and not from the relations of production. Power is in the form of knowledge and to control the flow of knowledge represents the greatest form of power. Due to this view of information flow as power, the hacker ethic of free information is seen as a balancing of power.

6.5 Hacking – The Legitimacy of Knowledge

The general argument that has been presented is that hackers represent a new group of powerbrokers in the information society. They exert their power by being at the centre of innovation and by carrying out illicit activities which influence how governments, corporations and consumers view the digital world. The public's perception is shaped by the media's presentation of the topic of hacking, in which the institutionalized corporate media frames the issue in the light of hackers as economic disrupters in conjunction with the sensationalistic tendencies creating a moral panic surrounding the phenomena. Regardless of how the media treat hackers, they are being integrated into the mainstream economy, both willingly on the part of hackers and on the part of employers. A central question remains unanswered; why? Why are hackers willing to discuss issues with corporations and governments?

It is my opinion that by applying Merton's theory of cultural adaptation, a clearer picture of what hacking really symbolizes emerges.

At the core of the hacker issue is a conflict between society's goal of individual innovation and the acceptable methods of demonstrating innovation, creativity and of acquiring knowledge. Due to the increasing immaterial nature of technology there has been an intensification in the patenting of information and the introduction of

technological impediments to transferring knowledge within the non-profit segment of society. Society establishes the goal of being technologically proficient while at the same time limits the potential of the individual to excel by using self-taught principles. Hacking is a rebellious movement intended to change the fundamental way in which society views technology and the relationship between producers and consumers of programmable goods. This rebellion includes elements of democratic control and a shifting of power from the producer to the consumer and reflects an alienation from the reigning culture and structure.

At the heart of the hacker argument is that the motivation for profit in the production of software has compromised the ability of producers to create innovative software. The closed process under which commercial software companies create products leads to inferior programs. Furthermore, the reliance on established sources of knowledge as the sole source of information has lead to stale technology. The open source software community, which is a manifestation of the hacker ethic and ideology, is at the forefront of the radical movement to change the way in which producers and consumers think about proprietary information.

Hackers form a movement that wants to be integrated into the information economy, but not the current one. For all the talk of the 'new' economy, the current system of production is the mirror

image of the industrial economy. The digital nature of products has not changed the way they are copyrighted, the way they are not shared nor has it changed the way collaboration means a team within one company devoid of interaction with the consumer. Hackers want to change the way society thinks about technology, who can use it, how they can use it, and for what purposes. Hackers want to change the means of acquiring knowledge and legitimize the way they gained their understanding of computers. Hackers also want to challenge the established goal of creating computer knowledge, which is profit.

Hacking is not simply an activity but rather encompasses a philosophy. The reason for the production of software is the process in and of itself. Breaking into networks is done because it can be. Hacking is a derivative of the greatest human qualities – that of curiosity and ingenuity – and represents a method of adaptation to certain social pressures such as the privatization of knowledge and the rapid introduction of new programmable technologies in society.

Hackers, as a social group openly criticize and reject the corporate goal of profit. In the zest to increase market share, commercial software production has lead to appealing to the lowest understanding of technology, which is the making of 'user friendly' products. The term 'user friendly' is a euphemism for making sure the consumer remains ignorant. The hacker movement is leading to the rise in the public's computer literacy in order to end their dependency

on the commercial software producers and products. Hackers essentially reject the creation of *users* of technology as their social project is the creation of *producers* of technology which they are attempting to create by fostering a better understanding of how computers function.

Hackers directly challenge the cultural means of acquiring and disseminating knowledge. Hackers seek knowledge from first hand exploration of technology and from others in the hacker community. School is generally rejected as a means of acquiring innovative knowledge. The legal parameters in which information is gathered is rejected as a whole as it is seen as an illegitimate barrier imposed by commercial software developers. Hackers are seeking legitimization of the means by which they acquire their knowledge and are seeking to influence the goal of software production, thus, falling within Merton's category of rebellion. They are attempting to change the hierarchical system of knowledge production by challenging the existing corporate order. By proving that software produced by hackers, using the hacker open-source methodology is superior to commercial development, hackers are challenging the foundation on which commercial companies base their authority. For this reason hackers can be seen as part of a rebellious social movement.

Questioning the relationship between producers and consumers brings into focus the issue of power. In the current

structure of production, the commercial software developers determine what will be produced, how it will be produced and what it may be used for. Circumventing technological barriers imposed by the corporate world enhances democratic relations by increasing the power of the consumer; the power to decide how to apply a product or to create a new one. Hacking is not simply about consumer choices between Microsoft and Apple, but rather, a choice between pre-packaged goods and the ability to create one's own tools and apply them in any way one so desires. Power over the destiny of the technology under one's control is a fundamental element of hacking and the hacker should be seen as of a rebel attempting to change the larger structure of the relationship between technology and the user. For this reason hackers have adapted to the pressures and limitations imposed by commercial software production by creating a rebellious movement.

6.6 Conclusion

The hacker phenomenon is complex including many dimensions. All of the element surrounding the issue of hacker influence on the market place, the way the media frames the hacker debate, the issue of hacktivism within the computer underground and finally as a method of rebellion, are complicated. In order to fully understand hacking a dialectical frame of reference must be utilized.

On the one hand, hackers are an integral part of the information economy, exerting influence on the production of new consumer products. On the other hand, hackers are considered marginal elements with no official place within the corporate hierarchy. They gain their power because of their innovation and their reputation for challenging the existing corporate structure within the field of software production. Yet this reputation is also problematic because it leads to a stigmatization as economic disturbers and has lead to their criminilization. While the media officially vilifies hackers, the public seems to be less inclined to demonize their activities. It is this cantankerous relationship between mainstream society and the marginal element of the computer underground that has lead to the creation of one of the most fascinating groups of the new economy – the hackers.

Chapter 7 – Conclusion

The goal of this study was to examine the phenomena of hacking and to determine whether it reflects a nihilistic activity with no other underlying goal than to wreak havoc upon society or whether there is a deeper meaning. Beginning with a review of existing literature to determine the missing elements of previous works, a definitional framework was established to articulate the meaning of hacking. The definition of a hacker used for this study was a computer enthusiast who has adopted the spirit of the hacker ethic and has the technical ability to circumvent technological barriers in order to create innovative technological artifacts. The philosophical underpinnings of the hacker ethic were examined which enabled the understanding of the observations of the hacker conference and the interpretation of the data gathered from the hacker list server. Following this, a discussion of how hackers represent the new powerbrokers in the information society and how their influence is exerted. Given the importance of the media in shaping the views of society, the precarious relationship that hackers have with mainstream media was also examined.

All of these elements contribute to a comprehensive understanding of hacking as a form of cultural adaptation to the pressures created by the free market in the field of software development. By applying Merton's theory of cultural adaptation to the phenomena of hacking, we are able to understand that hacking

represents an attack on the structure encompassing software production. The fundamental way in which knowledge is limited in the information age has become the target of the computer hacker who circumvents software copyrights and licensing schemes which are seen as illegitimate and repressive. Hackers can be considered a new category of social rebels. At the heart of hacking is the belief that all users of programmable technology possess the intellectual capabilities to become creators, if only an open atmosphere of knowledge sharing were a reality.

Although hacking is a rebellious activity, it is important not to confound a technological philosophy with a greater social project. Hackers come from different backgrounds and transcend national borders, which means that their material interests often conflict. For that reason, hackers have varied opinions about non-technological issues as demonstrated by the content analysis of the list server. The conflicting views make it impossible to say that hackers as a whole form a politically motivated group determined to change the relationships of power in greater society. Hacking is an activity related to technology and the way in which producers and users interact with one another in the creative process of software development. Politically like-minded hackers will group together for particular projects, however, hacking must always be seen as a technological pursuit.

Many have tried to explain what motivates hackers to do what they do. Addictive personalities, the sense of power over other machines or even the sense of importance gained from bragging rights from a particular exploit have all been suggested. I propose that the real answer to this question lies in the close relationship that computer hackers have with phone phreaking and lock picking. The barriers that inhabit the digital world have a relationship to the barriers in the material world and it is the human desire to understand how things work and how to improve upon them that motivates computer hackers and non-computer hackers alike. From the first Neolithic humans discovering the secrets of the wheel to the early astronomers and physicians mapping out the sky and the body, hackers follow a rich lineage of questioners and amateur technicians who have pushed the barriers of their time. Hacking is part of the human spirit of discovery and as such society will never be rid of the phenomena just as it has always existed in different forms. The word 'hacking' is simply the synonym for discovery in our new digital world.

Bibliography

Asimov, Isaac. Robots Visions. New York: ROC Publications, 1990.

Bell, Daniel. The Coming of Post-Industrial Society: A Venture in Social Forecasting. 3rd ed. New York: Basic Books, 1999.

Beniger, James R. The Control Revolution: Technological and Economic Origins of the Information Society. Cambridge: Harvard Press, 1986.

Blake, Scott. "Selling Out: The Pros and Cons of Working for the Man." H2K. Hackers On Planet Earth. Pensylvania Hotel, Jul. 14, 2000.

Braverman, Harry. Labor and Monopoly Capital: The Degradation of Work in the Twentieth Century. New York: Monthly Review Press, 1974.

Castells, Manuel. The Rise of the Network Society. England: Blackwell Publishers, 1996.

Chantler, Alan Nicholas. "Risk: The Profile of the Computer Hacker". Diss. Curtin University of Technology, 1995.

Chomsky, Noam. Detering Democracy. New York: Hill and Wang, 1992.

Chomsky, Noam. Necessary Illusions: thought conrol in democratic societies. Toronto: Anansi, 1989.

Clough, Bryan and Paul Mungo. Approaching Zero: Data Crime and the Computer Underworld. London: Faber & Faber, 1992.

Cohen, Stanley. Folk Devils and Moral Panics: The Creation of the Mods and Rockers. Oxford: Martin Robertson, 1980.

Cohen, Stanley. "Mods and Rockers: the inventory as manufactured News." The Manufacture of News. Ed. Stanley Cohen and Jack Young. London: The Anchor Press, 1973.

Dufresque, David and Florent Latrive. Pirates et flics du net. Paris: Éditions du Seuil, 2000.

"Fraude informatique." Host Jean-François Lépine. Zone Libre. Société Radio Canada, Nov. 4 1999.

Gibson, William. Neuromancer. New York: Ace Science Fiction, 1984.

Golding, Peter. "Global Village or Cultural Pillage? The Unequal Inheritance of the Communications Revolution" Capitalism and the Information Age: The Political Economy of the Global Communication Revolution Ed. Robert W. McChesney, Ellen Meiksins Wood and John Ballamy Foster 1998: 69-86 (75).

Goldstein, Emmanuel. "Lies." 2600: The Hacker Quarterly Vol. 15 No. 2 1998: 4-5, 54 (3).

Graphix, Mr. Ohm, Nightstalker, and Sam Nitzberg. "Retro Computing." H2K. Hackers On Planet Earth. Pensylvania Hotel, Jul. 15 2000.

Gutstein, Donald. E.Con: How the Internet Undermines Democracy. Toronto: Stoddart, 1999.

"Hacker Crackdown." Host Wendy Mesley. Undercurrents. Canadian Broadcasting Corporation, Jan. 18 1998.

Hackers. Dir. Iain Softley. Perf. Jonny Lee Miller, Angelina Jolie, and Fisher Stevens. Metro Goldwyn Mayer Studios, 1995

"Hackers." Host Rex Murphy. The Fifth Estate. Canadian Broadcasting Corporation, Dec. 6 2000.

Hafner, Katie and John Markoff. Cyberpunk: Outlaws and Hackers on the Computer Frontier. New York: Simon & Schuster, 1995.

Hannemyr, Gisle. "Technology and Pleasure: Hacking Considered Constructive" 1997. Jan. 25 2001 <http://home.sol.no/~gisle/oks 97.html>.

Herman, Edward S. and Noam Chomsky. Manufacturing Consent: the Political Economy of the Mass Media. Toronto: Randam House, 1988.

Himanen, Pekka. The Hacker Ethic and the Spirit of the Information Age. New York: Random House, 2001.

Jordan, Tim. Cyberpower: The Culture and Politics of Cyberspace and the Internet. New York: Routledge, 1999.

Jordan, Tim and Paul Taylor. "A Sociology of Hackers." INet 98 N. d. Jan. 25 2001 <http://fc.vdu.lt/Conferences/INET98/2d/2d_1.htm>.

Kroker, Arthur and Machael A. Weinstein. Data Trash: the theory of the virtual class. New York: St. Martin's Press, 1994.

Labrosse, Denis. "Hackers: La cyberculture à ses extrêmes." Diss. Université du Québec à Montréal 1999. Oct. 30 2000 <http://www.er. uqam.ca/nobel/ d124600/hackers/index.html>.

Levy, Steven. Hackers : Heroes of the Computer Revolution. New York : Delta Trade Paperbacks, 1994.

Littman, Jonathan. The Fugitive Game: Online with Kevin Mitnick. Boston: Little, Brown & Company, 1996.

Littman, Jonathan. The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen. Boston: Little, Brown & Company, 1997.

Markoff, John and Tsutomu Shimomura. Takedown: the pursuit and Capture of Kevin Mitnick the World's most Notorious Cybercriminal - by the Man who did it. New York: Hyperion, 1996.

McMahon, David. Cyber Threat: Internet Security for Home and Business. Toronto: Warwick Publishing Inc., 2000.

Merton, Robert K. Social Theory and Social Structure. Illinois: The Free Press, 1957.

Merton, Robert K. "Social Structure and Anomie." Social Theory and Social Structure 1976: 185-214 (39). Facstaff.bucknell.edu Apr. 5 2001 <http://www.facstaff.bucknell.edu/kendrick/soci211 /readings/ durkheim/contemporary/merton--anomie.html>.

Meyer, Gordon R. 1989. "The Social Organization of the Computer Underground." Socio.niu.edu 1989. Jan. 25 2001 <http://www. soci.niu.edu/theses/gordon>.

Mitnick, Kevin. "A Taste of Freedom." 2600: The Hacker Quarterly Spr. 2000 17 1: 9-11 (3).

Newby, Gregg. "The Hacker's Code." H2K. Hackers On Planet Earth. Hotel Pensylvania, New York. Jul. 16 2000.

Newby, Gregg. "The Hacker's Code: Draft." Gregg Newby's Personal

Home Page N. d. Aug. 27 2000 <http.unc.edu/gbnewby/code>.

Ogien, Albert. Sociologie de la deviance. Paris: Armand Colin, 1999.

Raymond, Eric S. "How To Become A Hacker." Tuxedo.org N.d. Dec. 7 2000 <http://www.tuxedo.org/~esr/faqs/hacker-howto.html>.

Raymond, Eric S. "The Cathedral and the Bazaar." First Monday.org 1998. Jan. 25 2001 <http://firstmonday.org/issues/issue3_3/ raymond/index.html>.

Raymond, Eric S. The New Hacker's Dictionary. Third Ed. Massachusetts: MIT Press, 1998.

Rifkin, Jeremy. La Fin du Travail. Quebec: Édition Boréal, 1996.

Robins, Kevin and Frank Webster. Times of the Technoculture: From the information society to the virtual life. New York: Routledge, 1999.

Rosteck, Tanja S. "Computer Hackers: Rebels With a Cause." Fortunecity 1994. Jan. 25 2001 <http://www.fortunecity.co.uk/ skyscraper/perl/620/ hacking.html>.

Ruffin, Oxblood. "Communications Presents: The L0pht Hurrah." Cult of the Dead Cow Aug. 4 2000. Feb. 27 2001 <http://www.cult deadcow. com/cDc_files/0374.html.>

Schwartau, Winn. Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption. New York: Thunder's Mouth Press, 2000.

Segaller, Stephen. Nerds 2.0.1: A Brief History of the Internet. Oregon: TV Books, 1998.

Slatalla, Michelle and Joshua Quittner. Masters of Deception:The Gang That Ruled Cyberspace. New York: Harper Perennial, 1995.

Sneakers. Dir. Phil Alden Robinson. Perf. Robert Redford, Sidney Poitier, Dan Aykroyd, River Phoenix, David Strathairn, Mary McDonnell, Ben Kingsley, and James Earl. Universal Studios, 1992.

Steele, Robert, Sam Nitzberg and Winn Schwartau. "Ethics in Military and Civilian Software Development." H2K. Hackers On Planet Earth. Pensylvania Hotel, New York. Jul. 14 2000.

Sterling, Bruce. The Hacker Crackdown: Law and Disorder on the Electronic Frontier. New York: Bantam, 1992.

Stoll, Clifford. The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage. New York: Doubleday, 1989.

Swordfish. Dir. Dominic Sena. Perf. John Travolta, Hugh Jackman, Halle Berry, Don Cheadle and Vinnie Jones. Warner Brothers, 2001.

Taylor, Paul A. Hackers: Crime in the digital sublime. New York: Routledge, 1999.

The Lone Gunmen. Dir. Bryan Spicer. Perf. Tom Braidwood, Dean Haglund, and Bruce Harwood. Fox Network, 2001.

+he Mentor. "The Hacker's Manifesto." Demonstreet.com 1986. Feb. 27 2001 <http://www.demonstreet.com/hacking/mentor.htm>.

The Net. Dir. Irwin Winkler. Perf. Sandra Bullock, Jeremy Northam, Dennis Miller, Diane Baker, Wendy Gazelle, Ken Howard, and Ray McKinnon. Columbia Tristar, 1995.

Thurow, Lester C. The Future of Capitalism: How Today's Economic Forces Shape Tomorrow's World. New York: Penguin Books, 1997.

Toffler, Alvin. Future Shock. New York: Bantam Books, 1971.

Touraine, Alain. La société post-industrielle. Paris: Éditions Denoël, 1969.

"True Life: I am a hacker." Perf. Mantis and Shamrock. True Life. Music Television (MTV), Oct. 10, 1999.

Wargames. Dir. John Badham. Perf. Matthew Broderick, Dabney Coleman, John Wood, and Ally Sheedy. Metro Goldwyn Mayer Studios, 1983.

Wignall, Jonathan "Being A Good Samaritan Online." H2K. Hackers On Planet Earth. Hotel Pensylvania, New York. Jul. 16 2000.

Vallopillil, Vinod. "Open Source Software: A (New?) Development

Methodology." OpenSource.Org Ed. Eric S. Raymond Nov. 1998. Jan. 4 2001 <http://www.openresources.com/documents/halloween-1/>.

News Articles

Allair, D. Letter. "Hiring Hackers." CIO.COM. N. d. Jan. 4 2001 <http://comment.cio.com/sound _see_comments.cfm?ID=2387>.

"Alleged CNN hacker faces more charges." The Globe and Mail Online. Aug. 4 2000. Nov 28 2000 <http://globeandmail.com>.

"Anti-globalist protesters turn online." Globe and Mail Online Feb. 8 2001. Feb. 2 2001 <http://www.globeandmail. com/serle...=20010208&archive=rtgam&site=front>.

Appleyard, Kristen. "Hackers spark security upgrade: Holland Internet provider victim of an obscene page switch." The Holland Sentinel: On-line Edition Oct. 25 1997. Aug. 4 2001 <http://www.thehollandsentinel.net/stories/102597/new_hacker.html>.

Auster, Joel. "Vieux hackers à cran: Leur convention annuelle laisse percer un conflit de generation." Le Devoir Aug. 7 2000: B3.

Boswell, Randy. "'Hacktivism' is OK, professor says." The Ottawa Citizen 29 Mar. 2001: C7.

Bradham, Tom. Letter. "Hiring Hacker." CIO.COM N.d. Jan. 4 2001 <http://comment.cio.com/sound _see_comments.cfm?ID=2400>.

Callaway, Erin. "Ethical Hackers for Hire." ZDNet Jan. 7 1997. Aug. 1 2001 < http://www5.zdnet.com/zdnn/content/pcwk/1404/cwk0082.html>.

Campbell, K.K. "Bloodaxe Comes Out Swinging: Phrack editor Chris Goggans on Masters of Deception." Kkc.net Aug. 31 19995. Feb. 28 2001 <http://www.kkc.net/eyenet/1995/net0831.htm>.

Canlas, Ruben D. "Cookies Help." Happy Hacker Digest Mar. 1 1997. Jul. 24 2001 <http://w1.340.telia.com/~u34002171/hhd/1997/hhdmar1.html>.

Carter, B.J. Letter. "Hiring Hacker." CIO.COM N.d. Jan. 4 2001 <http://comment.cio.Bcom/sound_see_comments.cfm?ID=2408>.

Christensen, John. "Insurgency on the Internet: Bracing for guerrilla

warfare in cyberspace." CNN Online Apr. 6 1999. Feb. 21 2001 <http://www.cnn.com/tech/specials/hackers/cyberterror>.

"Could You Pass The Tiger Test?" The Guardian Online Mar. 9 2000. Aug. 1 2001 <http://www.guardian.co.uk/online/story/0,3605, 235346,00.html>.

Couvelaire, Anne-Louise. "Guerre Économique: Les 'espions' du troisième type." Le Nouvel Observateur Jan. 6 2000: 34-36.

Del Grosso, David. Letter. "Hiring Hackers." CIO.COM N. d. Jan. 4 2001 <http://comment.cio.com/sound _see_comments.cfm? ID=2588>.

Delong, Daniel F. " Hackers Said To Cost U.S. Billions." News factor.com Feb. 8 2001. Aug. 4 2001 < http://www.newsfactor. com/perl/story/7349.html>.

Eudes, Yves. "Au malheur des chasseurs." Le Monde Oct. 27 2000: 16.

Evenson, Laura and Michelle Quinn. " The Downfall of a Computer Wiz / How a lonely misfit became the FBI's most-wanted hacker." San Fransisco Chronicle Online Nov. 17 1995. Aut. 4 2001 <http://www.sfgate.com/net/hacker/sfc20217.html>.

"Federal Cybercrime Unit Hunts for Hackers." New York Times Online Jun. 2 1999. Nov. 28 2000 <Http://nytimes.com.>

FMStut. Letter. "Let's get the analogies right..." CIO.COM N. d. Jan. 4 2001. <http://comment.cio.com/sound_see_ comments. cfm?ID=2411>.

Ford, Fred. "Capitalism's newest enemies – computer nerds." The Ottawa Citizen Apr. 8 2001: C4.

Fridman, Sherman. "Hack Attacks Inherent to E-business – Experts." Newsbytes Online Feb 17 2000. Apr. 4 2001 <http://www.news bytes. com/pubnews/00/144089.html>.

"Frontline: Hackers." Public Broadcasting Station N.d. Jun. 31 2001 <http://www.pbs.org/wgbh/pages/ frontline/shows/hackers/ interviews/curador.html>.

Geralds, John. " Hackers cost firms billions of dollars." Vnunet.com

Oct. 8 2001. Aug. 4 2001 <http://www.vnunet.com/News/1117559>.

Glasner, Joanna. "Cracking for the man." Wired News Sep. 23 1999. Aug. 1 2001 < http://www.wired.com/news/business/0,1367,21879,00.html>.

"Hackers could threaten U.S. skies." ZDNet News Sep. 27 2000. Nov. 28 2000 <http://www.zdnet.com>.

Haselton, Bennett and Jamie McCarthy. "Internet Explorer 'Open Cookie Jar': Cookies storied by IE for Windows can be read by any Web site." Peacefire.org May 11 2000. Jul. 24 2001. <http://peacefire.org/security/iecookies/>.

Hellner, Martha. "Would You Hire a Hacker?" CIO.COM N.d. Jan. 4 2001 <http://comment.cio.com/sound.cfm?ID=50>.

Hogan, Mike. "Hacker attacks: You can never be too safe." CNN.com Nov. 1 2000. Apr. 4 2001 <http://www.cnn.com/2000/tech/computing/11/01/security.hackers.idg>.

Hulme, George V and Tony Kontzer. "Vulnerabilities Beckon Some With A License To Hack – Companies must consider legal ramifications, along with ethics, when they hire hackers." Techweb.com Oct. 3 2000. Jan. 4 2001 <http://www.techweb.com/se/_directlink.cgi ?IWK20001023S0072>.

"IBM Hires Out 'Hacker' Team As Security Force." ZDNet News Mar. 23 1998. Jan. 30 2001 <http://www.zdnet.com/zdnn/content/reut/0323/296845.html>.

"Insurgency on the Internet: Q & A with Emmanuel Goldstein of 2600: The Hacker's Quarterly." CNN Online N. d. Feb. 21 2001 < http://www. cnn.com/tech/specials/hackers/quandas/goldstein.html>.

"Insurgency on the Internet: Q & A with IBM's Chales Palmer." CNN Online N. d. Feb. 21 2001 < http://www.cnn.com/tech/specials/hackers/quandas/goldstein.html>.

Irwin, Roger. "What is FUD?" OpenSource.org 1998. Mar. 12 2001 <http://www.geocities.com/Silicon Valley/Hills/9267/fuddef.html>.

Jackson, William. "Feds come out from hiding at hacker show." Government Computer News Aug. 7 2000 v19 i22: p7(1).

Jackson, William. "Feds reach out to hacker community." Government Computer News, Jul. 26 1999 v18 i23: p73(1).

Jones International. "Computers: History and Development." Jones Telecommunications & Multimedia Encyclopedia 1994. Jul. 7 2001 <http://www.digitalcentury.com/encyclo/update/comp_hd.html>.

Kadar, Mike. Letter. "Hiring Hackers." CIO.COM N. d. Jan. 4 2001 <http://comment.cio.com/sound_ see_comments.cfm?ID=2392>.

Konrad, Rachel. "Hack attacks a global concern." CNet News.com Oct. 29 2000. Apr. 4 2000 <http://news.cnet.com/news/0-1003-200-3314544.html>.

Kubala, Tom. Letter. "Hackers Add Diversity to IT." CIO.COM N. d. Jan. 4 2001 <http://comment.cio.com/sound_see_comments .cfm?ID=2394>.

"Le coût de piratage informatique en hausse de 42% aux États-Unis." Cyberpresse.ca Mar. 12 2000. Mar. 13 2001 <http://www. cyberpresse.ca/groups/public/documents/convertis/puba_p1041642 .hcsp>.

Lange, Larry. "Trust a hacker under 30? You'd better." Electronic Engineering Times, Aug. 19 1996 915: p. 4 (2).

Latrive, Florent. "L'Europe envoie un hacker réguler le web." Libération, Oct. 12 2000 : p. 33.

Legard, David. "Hackers hit U.S., U.K., Australian government sites." Europe.cc.com Jan. 22 2001. Apr. 4 2001 <http://europe.cc.com/ 2001/tech/computing/ 01/22/government.hackers.idg, january 22, 2001>.

Lemos, Robert. "Start-ups offers $10,000 reward to hackers." ZDNet News Apr. 2 2001. Apr. 3 2001 <http://www.zdnet.com/zdnn/ stories/news/ 0,4586,5080549,00.html>.

Ludlow, Mark. "Professional Hacker for Hire." Inforwar.com Apr. 19 1999. Jan. 8 2001 <http://www.infowar.com/hacker/99/hack _041999a_j.shtml>.

Mandeville, David. "Insurgency on the Internet: Hackers, crackers and Trojan horses: a primer." CNN.com Mar. 29 1999. Mar. 21 2001 <http://www.cnn.com/tech/specials/hackers/primer>.

Mann, Charles C. "The Heavenly Jukebox." The Atlantic Monthly Sep. 2000: pp. 39-59.

McFedries, Paul. "The Word Spy." Logophilia.com Feb. 8 2001. Apr. 9 2001 <http://www.logophilia.com/wordspy/whitehathacker.html>.

McGuire, David. "Cyber Terrorism Serious Threat." Computer User Oct. 10 1999. Apr. 4 2001 <http://www.computeruser.com/ newstoday/99/10/10news6.html>.

Merritt, James W. "IMHO: Need Security? Get A Real Expert." Informationweek.com Apr. 3 2000. Jan. 4 2001 <www.information week.com/780/80uwjm.htm>.

Nair-Ghaswalla, Amrita. "India: Licensed To Bill – 'Ethical Hackers' Get Paid To Crack E-security." Inforwar.com May 23 2000. Jan. 8 2001 <http://www.infowar.com/hacker/00/hack_052300b_j.shtml>.

Neighly, Patrick. "Meet the Hackers." America's Network Jun. 1 2000. Apr. 4 2001 <http://www.americasnetwork.com/issues/2000issues/ 20000601/20000601_hackers.htm>.

New Republic. "The Editors: To Our Readers." The New Republic Jun. 1 1998. Apr. 9 2001 <http://magazines.enews.com/ magazines /tnr/current/ourreaders060198.html>.

Niehaus, John. "Web seal securing business." Dayton Business Journal Feb. 9 1998. Aug. 10 2001 <http://dayton.bcentral.com/ dayton/stories/1998/02/09/story6.html>.

Noack, David. "The Back Door Into Cyber-Terrorism." APBnews.com Jun. 2 2000. Apr. 4 2001 <http://www.apbnews.com/newscenter/ internetcrime/2000/06/02/ computerholes0602_01.html>.

Null, Christopher. July 2000. "How to Hire a Hacker." Smart Business: For The New Economy Jul. 2000: 112-118 (7).

Open Source Initiative. "The Open Source Definition." OpenSource. Org 1.8. Mar. 12 2001 <http://www.opensource.org/docs/ definition_plain.html>.

Penenberg, Adam L. "Forbes smokes out fake New Republic Story on Hackers." Forbes.com May 11 1998. Apr. 9 2001 <http://www. forbes.com/1998/05/11/otw.html>.

Petrella, Riccardo. "La Mondialisation de la technologie et de

l'économie. Une (hypo)these prospective." Futuribles Sep. 1989 135: 3-25 (23).

Petruzel, Oliver. Letter. "Hiring a Hacker." CIO.COM N.d. Jan. 4 2001 <http://comment.cio. com/sound_see_comments. cfm?ID=2421>.

Platt, Charles. " Hackers: Threat or Menace?" Wired.com Nov. 1994. Aug. 4 2001 <http://www.wired.com/wired/archive/2.11/hack .cong_pr.html>.

"Pricewaterhouse Coopers Warns Against Hackers-As-Security-Consultants Trend; Four Keys To Hiring An 'Ethical Hacker'." IT Security.com Jun. 14 2000. Jan. 4 2001 <http://www.itsecurity. com/jun2000/june14.htm>.

Reuters. "Hacker attacks expected over New Year's weekend." Boston Herald.com. Dec. 30 2000. Jan. 21 2001 <http://www. bostonherald.com/business/technology/hack12302000.htm>.

Roberts, Walt. Letter. "Talkback Central." ZDNET News N.d. Mar. 4 2001 <http://www.zdnet.com/tlkbck/comment/22/0,7056,109267-770104,00.html>.

Roush, Wade. "Hackers: Taking a Byte Out of Computer Crime." Technology Review Apr. 1995. Apr. 4 2001 <http://209.58.177.220/ articles/apr95/ roush.html>.

Rose, Barbara. "Copycat hacker attacks expected now, experts Predict." Fox News Online Jan. 26 2001. Apr. 4 2001 < http://sns. fox61.com/technology/sns-microsoft.story?coll=sns-technology-headlines>.

Ross, Jen. "Canada called 'hacker heaven' for criminals." Globe and Mail Online May 17 1999. Apr. 4 2001 <http://www.efc.ca/ pages/media/globe.17may99b.html>.

Royal Canadian Mounted Police. "What is computer crime?" Royal Canadian Mounted Police N.d. Jun. 31 2001 <http://www. netaccess._on.ca/_~rcmpham/computer.htm>.

Sales, Leigh. "Computer experts are warning cyber-terrorism could strike the Sydney Games." ABC News. Sep. 9, 2000. Jan. 4 2001 < http://www.abc.net.au/news/olympics/studio2000.htm>.

Schorow, Stephanie. "Cutting to the chase: Hackers join forces with

security firm to keep the world safe." Boston Herald Jan. 18 2000. Apr. 4 2001 <http://www.bostonherald.com/bostonherald/life/net01182000.htm>.

Seminerio, Maria. "Support grows for Pentium III protest." ZDNet.news Apr. 8 1999. Jul. 31 2001 <http://www.zdnet.com/zdnn/stories/news/0,4586,2238595,00.html>.

Solomon, Norman. "What Happened to the 'Information Superhighway?'" Z Magazine Feb. 2000: 11-13 (3).

Stone, Martin. "Hackers Mar 26 Government Sites." Newsbytes Jan. 23 2001. Apr. 4 2001 <http://www.newsbytes.com/news/01/160877.html>.

Sullivan, Bob. "Hackers amas new zombie army." MSNBC.com Sep. 15 2000. Apr. 4 2001 <http://wwww.msnbc.com/news/460824.asp?cp1=1>.

Sullivan, Bob. "Hacker diaries: How crooks milk the system." ZDNet News Apr. 2 2001. Apr. 3 2001 <http://www.zdnet.com/zdnn/stories/news/0,4586, 2703351,00.html>.

Taylor, Chris. "Cracking the Code.", Time Magazine Online Mar. 1999. Mar. 21 2001 <http://www.time.com/time/digital/feature/0,2955,22 179,00.html>.

Theall, George A. "What is a Computer Virus." Thomas Jefferson University Computer Virus Information Page N. d. Jun. 24 2001 <http://www.tju.edu/tju/dis/virus/>.

Thomas, Douglas. "Hacker Stereotypes: The Glass Menagerie." Online Journal of Reporting May 20 1998. Apr. 9 2001 <http://ojr.usc.edu/content/ print.cfm?print=45>.

"Tout, vous saurez tout sur le cookie." L'Internaute.com N. d. Jul. 24 2001 <http://www.Linternaute.com/surfer /cookie/ cookiesomm .shtm>.

Walton, David. "Insurgency on the Internet: Scenes from a mall." CNN online Mar. 29 1999. Mar. 21 2001 <http://www.cnn.com/tech/specials/hackers/culture>.

Wasserman, Elizabeth. "Feds take steps against threat of cyber Terrorism." CNN.com Sep. 25 1998. Apr. 4 2001 <http://www.cnn.com/tech/computing/9809/25/ cyberterrorism .idg >.

Weston, Randy. "Microsoft profits from license changes." CJNET News.com Sep. 4 1998. Jul. 31 2001 <http://news.cnet.com/news/0,10000,0-1003-200-332915,00.html>.

Windrem, Robert and Jim Miklaszewski. "Pentagon and Hackers in 'Cyberwar'." MSNBC Mar. 5 1999. Jul. 8 2000. < http://www.zdnet.com/zdnn/stories/news/0,4586,2220773,00.html>.

York, Geoffrey. "The Internet's Zen Pirates." Globe and Mail Dec. 6 2000. Dec. 17 2000 <at: http://archive.theglobeandmail. co... esultstart%3d1%26resultcount%3d10&>.

Zetter, Kim. "Hacker Nation." PCWorld.com May 2001. Jul. 4 2001 <http://www.pcworld.com/features/article/0,aid,44544,00.asp>. Jan. 8 2001 <http://www.pcworld.com/resource/printable/article/0,aid, 44544,00.asp>.

Web Site

2600: The Hacker Quarterly <Http://www.2600.com>.

@Stake <http://www.atstake.com/>.

Attrition.Org <http://www.attrition.org/>.

Comsec <http://www.comsec-solutions.com/>.

Cult of the Dead Cow <Http://www.cultdeadcow.com/>.

Defcon <http://www.defcon.org>.

Electrohippies <http://www.gn.apc.org/pmhp/ehippies/high-index.html>.

Electronic Frontier Foundation <Http://www.eff.org/>.

Hacker News Network <Http://www.hackernews.com/>.

Phrack Inc <Http://www.2600.com/phrack/>.

The L0pht <Http://www.l0pht.com>.