Hackers:
A Case-Study of the Social Shaping of Computing

Paul Anthony Taylor

PhD
University of Edinburgh
1993

I hereby certify that the following PhD thesis was composed solely by myself. In addition, the thesis is completely my own work, subject only to the professional advice of my official doctoral supervisors.

ABSTRACT

Hackers: a case-study of the social shaping of computing

The study is an examination of hacking, placing the act in the context of theories of technological change. The account of hacking is used to substantiate those theories that emphasise the societal shaping of technology over the notion of technological determinism. The evolution of hacking is traced, showing how it reflects changing trends in the nature of information: the most vivid of these is the conceptualisation of information known as 'cyberspace'. Instead of simply cataloguing the impact of technical changes within computing, and the effects they have had upon information, the study shows how technical change takes place in a process of negotiation and conflict between groups.

The two main groups analysed are those of the Computer Underground (CU) and the Computer Security Industry (CSI). The experiences and views of both groups are recounted in what constitute internalist and externalist accounts of hacking and its significance. The internalist account is the evidence provided by hackers themselves. It addresses such issues as what motivates the act of hacking; whether there is an identifiable hacking culture; and why it is almost an exclusively male activity. The externalist account contains the perceptions of hacking held by those outside the activity.

The state of computing's security measures and its vulnerability to hacking is described, and evidence is provided of the extent to which hacking gives rise to technical knowledge that could be of potential use in the fixing of security weaknesses. The division within the CSI between those broadly cooperative with hackers and those largely hostile to them is examined, and the reasons why hacking knowledge is not generally utilised are explored. Hackers are prevented from gaining legitimacy within computing in a process referred to as 'closure'. Examples include hackers being stigmatised through the use of analogies that compare their computing activities to conventional crimes such as burglary and tresspass. Stigmatisation is carried out by the CSI who use it in a process of professional boundary formation to distinguish themselves from hackers. It is also used by other authority figures such as Members of Parliament whose involvement in the process of closure takes the form of the anti-hacking legislation they have passed, an analysis of which concludes this study.

Acknowledgements

Big thanks to everyone who helped me with this project at Edinburgh University's Research Centre for Social Sciences: to my supervisors Robin Williams and Rob Procter, who did the bulk of the academic spade-work with their invaluable advice - both on and off the pitch! to Wendy for all her suggestions along the way; and to Alf and Barbara for their friendly banter and encouragement.

Thanks to the friends who helped me trudge along: my closest friend - my sister, Christine; Jag and Alan the night-time babysitters; Matt for his advice; and especially Andy "Sadman" Snell and Hank "How many aircraft carriers have you got?" Mescall, who in their very different ways proved great mates.

Special love to the longest suffering victim of the thesis: Kate "Leeds! Leeds! Leeds!" Halloran who came off the bench in the second half to score a glorious equaliser to make it PhD 1 Relationships 1.

My heartfelt thanks to Professor Stell, the dedication and skill he showed after our first inauspicious meeting made this work physically possible: words can't express the debt owed to him by countless people.

Finally, the greatest love and thanks to the person to whom this work is dedicated: my father, Richard Daniel Taylor.

Acknowledgements

Chapter outlines

Chapter 1	Introduction	1
Chapter 2	Methodology	18
Chapter 3	Hackers: theories of technological change and the changing nature of information	29
Chapter 4	The hacking community: motivation and culture	73
Chapter 5	State of the industry: hawks and doves	125
Chapter 6	'Them and us'	180
Chpater 7	Hacking and legislation	230
Chapter 8	Conclusion	279
Appendix 1 -	Statistical analysis	300
Appendix 2 -	Glossary of terms and hacking case-studies	323
References		330
List of Interviews		338
List of Abbreviations		343

Chapter 1 - Introduction

1.1 INTRODUCTION
1.1.1 The definition
1.1.2 Key concepts
(i) constituencies
(ii) closure

1.2 THE IMPORTANCE OF HACKING

1.3 RESEARCH QUESTIONS
(i) Hackers and technological determinism
(ii) Hackers' counter-culture status.
(iii) Boundary formation
(iv) Stigmatisation
(v) Policy issues

1.4 SCOPE OF THE STUDY

1.5 OUTLINE OF CHAPTERS

Chapter 2 - Methodology

2.1 INTRODUCTION

2.2 CHOICE OF RESEARCH METHODS AND INSTRUMENTS

(i) Interviews

(ii) Method of contact

(iii) Sampling and representativeness

2.3 ADVANTAGES AND DISADVANTAGES OF E-MAIL AS A METHODOLOGICAL TOOL

2.3.1 Advantages

(i) Costs and space.

(ii) Speed and interactive nature

(iii) Increased response rate

2.3.2 Disadvantages

(i) Absence of regulating feedback

(ii) Validity

2.4 SPECIFIC E-MAILING TECHNIQUES

(i) Mailing-list targeting.

(ii) Personalisation of all correspondence

2.5 CONCLUSION

Chapter 3 - Hackers, theories of technological change and the changing nature of information

3.1 INTRODUCTION

3.2 TECHNOLOGICAL DETERMINISM

3.3. HACKERS AND TECHNOLOGICAL DETERMINISM

3.4 TECHNOLOGICAL POLITICS

3.5 LATOUR AND THE PRINCE
(i) Inertia
(ii) Automatism
3.5.1 Hackers and the Prince

3.6 THE CHANGING ECONOMIC NATURE OF INFORMATION

3.7 CYBERSPACE - THE REAL AND VIRTUAL WORLDS
3.7.1 Cyberspace and technological domination
(i) Domination of the individual
(ii) Cyberspace and technological determinism
3.7.2 Cyborgs: a rejection of technological determinism
3.7.3 Cyberspace and the culture of opposition

3.8 HACKING AS AN ALTERNATIVE CULTURE
3.8.1 Opposition to commodification
3.8.2 Hacking as anti-bureaucratic rebellion
3.8.3 Anti-Government sentiment - privacy and double standards

3.9 CONCLUSION

Chapter 4 - The hacker community: culture and motivation

4.1 INTRODUCTION
4.1.1 The hack
4.1.2 The hacker ethic

4.2 HACKING CULTURE
4.2.1 Hacking culture - specific elements
(i) Technology content
(ii) Secrecy
(iii) Anonymity
(iv) Fluidity of boundaries and speed of change
4.2.2 Hacking culture - Male predominance
4.2.3 Reasons for paucity of female computer scientists
(i) Societal Factors
(ii) The masculine environment
(iii) Gender in language
(iv) Hacking and the role of sexuality
(v) Hacking and machismo

4.3 ACADEMIC MOTIVATION THEORIES

4.4 HACKERS' MOTIVATION THEORIES
4.4.1 Feelings of Addiction
(i) Fieldwork evidence
(ii) The Bedworth case
4.4.2 Curiosity- humans and technology
4.4.3 Boredom
(i) Lack of mental stimulation
(ii) Lack of access
4.4.4 Enjoyment of feelings of power -information for information's sake
4.4.5 Peer recognition

4.5 CONCLUSION

Chapter 5 - State of the industry: hawks and doves

5.1 INTRODUCTION

5.2 THE EXISTENCE OF SECURITY WEAKNESSES
5.2.1 Qualitative evidence and the knowledge gap
5.2.2 Statistical evidence
5.2.3 Quantitative questionaire data

5.3 REASONS FOR SECURITY FLAWS
5.3.1 The Software Crisis
5.3.2 The Software crisis and the origins of hacking
5.3.3 The problem of anticipation and the role of testing
(i) Serendipity and intrinsic insecurity
(ii) State of computer security education
(iii) Calls for hands-on experience
5.3.4 The knowledge gap
5.3.5 Commercial pressures and security holes
(i) Job structure
(ii) Low profile of security
(iii) The constant need to update
(iv) The problems of updating: the responsibility of the vendor
(v) The exaggerated claims of marketing
(vi) Apathy and hype

5.4 THE RATIONALE FOR HACKERS
(i) The potential for cooperation
(ii) The industry benefit argument
(iii) Potential underestimation of the role of hackers

5.5 RATIONALE FOR NON-COOPERATON 'THE HAWKS'
(i) Technical arguments against cooperation
(ii) The question of trust - the case of Robert Schifreen

5.6 CONCLUSION

Chapter 6 - 'Them and Us'

6.1 INTRODUCTION

6.2 BOUNDARY FORMATION - 'THEM AND US'
6.2.1 The evidence - hawkish strength of feeling

6.3 REASONS FOR 'THEM AND US'
6.3.1 Ethical differences between the CSI and CU
6.3.2 The fear of anonymity

6.4 THE ETHICAL BASIS OF THE 'THEM AND US' SCENARIO
6.4.1 Blurred and vestigial ethics
6.4.2 Industry examples of blurred ethics
6.4.3 Technology and ethics

6.5 BOUNDARY FORMATION - ROLE OF THE MEDIA
(i) 'Hacker best-sellers'
(ii) Press and television

6.6 BOUNDARY FORMATION PROCESS AND THE USE OF ANALOGIES
(i) Analogies - property issues
(ii) Analogies - breaking and entering
(iii) The CU'S rejection of breaking and entering analogies
(iv) Problems of using analogies as explanatory tools - the hacker as cowboy

6.7 THE PROJECT OF PROFESSIONALISATION
6.7.1 Creation of the computer security market and professional ethos
6.7.2 Witch-hunts and hackers
6.7.3 Closure - the evolution of attitudes

6.8 CONCLUSION

Chapter 7 - Hacking and Legislation

7.1 INTRODUCTION

7.2 CLASSIFICATIONS OF COMPUTER CRIME

7.3 CRIMINAL ACTIVITIES OF HACKERS

7.4 PRESSURES TO CRIMINALISE

7.5 'SYMBOLIC LEGISLATION'

7.6 THE PARLIAMENTARY DEBATE
(i) Stigmatisation and analogies
(ii) The information gap

7.7 ISSUES IN COMPUTER MISUSE LEGISLATION
(i) Interpretations of motivation
(ii) Non-applicability of concepts in cyberspace
(iii) Deterrence aims
(iv) Symbolic value

7.8 PROBLEMS OF ENFORCEMENT
(i) Problems of enforcement
(ii) Legal complexities - the Bedworth case

7.9 LEGISLATION AND THE EVOLUTION OF HACKING: MIT TO ALCATRAZ

7.10 CONCLUSION

Chapter 8 - Conclusion

8.1 INTRODUCTION - THEMES OF THE STUDY

8.2 CONTRIBUTION TO EXISTING LITERATURE AND NOVELTY

(i) Contribution to hacking literature

(ii) Empirical novelty

8.3 SUMMARY OF FINDINGS - STATUS OF ORIGINAL RESEARCH QUESTIONS

(i) Hackers and technological determinism

(ii) Hackers counter-culture status - internalist vs externalist accounts

(iii) Boundary formation

(iv) Stigmatisation

(v) Policy implications

8.4 CONTRIBUTION TO THEORETICAL KNOWLEDGE

8.5 UNANSWERED QUESTIONS - FUTURE RESEARCH

Chapter 1 - Introduction

1.1 INTRODUCTION
1.1.1 The definition
1.1.2 Key concepts

1.2 THE IMPORTANCE OF HACKING

1.3 RESEARCH QUESTIONS

1.4 SCOPE OF THE STUDY

1.5 OUTLINE OF CHAPTERS

1.1 INTRODUCTION

This thesis is an analysis of the recent phenomenon of computer hacking; that is, the unauthorised access to and subsequent use of other people's computer systems. Hackers have evolved from a position of being instrumental in the development of the first computer programs, to their present status as a marginalised underground group. The analysis is used as a rebuttal of technological determinism by showing how computing affects society, as a result of the negotiations and conflicts of its interested groups, rather than due to any inherent logic of the technology itself.

Technological determinism encompasses the widespread perceptions which see technological development as being on an inevitable and autonomous trajectory. Such perceptions view technology as a 'black box'; the effects of technology are felt, but the means by which such effects are achieved are too complex to fathom or control. It is a notion that particularly applies to computers. Their literally box-like structure contains a machine that exhibits great computational power by virtue of its 'mysterious' manipulation of binary 1/0 inputs in the form of alternating electrical impulses.

The study is part of a tradition of technology studies known as the 'Social Shaping of Technology'. It explores the way in which technological development has a large socially-determined element, rather than being exclusively the result of autonomous technical processes. Bijker and Pinch describe this commonly-shared aim of social theories of technological change as, "The development of an empirically sensitive theoretical understanding of the processes by which sociotechnologies are shaped and stabilized". (Bijker and Pinch 1992: 13) It will be argued that hacking represents an illustration of the way in which technology is both "socially shaped" and "stabilised", phrases used by social theorists to denote the manner in which various groups within society contribute, by their negotiations and conflicts, to the eventual shape a technology takes, and which may then prove resistant to further socially-induced changes. These

theories are at pains to emphasise that technology is not a 'black-box' of effects produced by unknown causes; rather, the impact of a technology is but a reflection of a whole series of political and economic choices made by groups closely related to the development of the technology. Hackers constitute one such group in the historical development of computing: they illustrate a group of actors whose values oppose those of the dominant social order and who seek to shape computing to their own purposes.

1.1.1 The definition of hacking

In order to give a fuller idea of the various shades of meaning that lie behind the phrase hacking, various definitions of hacking activities are expanded upon in Appendix 2. There is no definitive description of what hackers and hacking are; the fact that it has disputed meanings and connotations for different groups is addressed as part of the study's analysis of group boundary formation within computing. Throughout this study the term will be used largely to refer to the unauthorised access to a computer system, or the information it contains. The term has gone through several changes from its original dictionary definition: of "cut or chop roughly; mangle: cut (one's way) through thick foliage etc.: manage, cope with": to its present definition of: "gain unauthorised access (to data in a computer)" [The Concise Oxford Dictionary 8th edition]. It has also evolved from the MIT days of the 1950's onwards when it was first used in the context of computing. The phrase was originally used to denote the highly skilled but largely playful activity of academic computer programmers searching for the most elegant and concise programming solution to any given problem (Levy 1984). It has since been increasingly associated with its present-day connotation of illicit computer intrusion.

The study traces the reason for this evolution in the meaning of the term and shows it to be part of a process by which hackers have been marginalised within computing; a process which is described as 'closure'. The reason why the phrase hacking came to be used in the

first place is possibly a reflection of the development of programming. The various connotations of the phrase have resonance with the problems encountered with programming the early computers, described by Levy (1984) as 'great hulking brutes'. These valve-based machines were notoriously unreliable, a factor which, combined with the relative immaturity of programming methods, led to solutions to any particular computing problem being rather haphazardly constructed, thus meeting the phrase's first connotation of something being fashioned roughly: being 'hacked together'. The baroque complexity and unmanageability of the early systems can also be associated with the connotations of 'managing or coping with' and 'cutting through thick foliage'.

In addition to 'hacker' there is also the more specific term 'cracker' which is more consistently and pejoratively used to describe someone who breaks into systems, often causing deliberate damage. This study will use the general word 'hacker' as an umbrella term for the various shades of meaning associated with the phrase. One of the purposes of the study itself is to highlight the amorphous nature of the term, and by extension, the activity.

1.1.2 Key Concepts

i) Constituencies

This concept is defined as:

> ensembles of institutions interacting with each other through and within the development of specific technologies ... Sociotechnical constituencies actually materialize technological processes in such a way that the fruits of these processes ... are moments of crystallizations of the workings of the constituency. Seen in this manner, the creation, production and diffusion of a given technology becomes a single process of interpenetration of technical, socioeconomic, political and cultural factors (Molina 1989a: 4).

Despite the fact that there may be several sociotechnical constituencies in the overall constituency of a particular technology, certain groups obtain a dominant status. In his study Molina defines the dominant social constituency as "the social forces which have in practice exercised the dominant control of the basic human, financial, material, time and space resources necessary for all technological processes, and which, for the same reason, have most directly influenced and shaped the development of microtechnology" (Molina 1989 a: 4).

In order to conceptualise the impact of social groups upon this study on the specific technology of computing, a framework is used that describes the overall constituency of computing as containing smaller 'sociotechnical constituencies'. This thesis investigates the main sociotechnical constituencies relevant to hacking - the Computer Underground (CU), the Computer Security Industry (CSI), and the academia-based computer users who are often found to straddle the two other groups. The study highlights the role of the non-dominant group of hackers within computing and illustrates from its investigation of their activity how local groups shape one particular aspect of a technology: in this case, computer security.

ii) Closure

Within the context of the heterogeneous influences upon a technology's development, dominant interests tend to emerge. Groups within a technological constituency adopt strategies aimed at limiting the influence of competing groups. Bijker and Law state that: "these are designed in all cases to box in the opposition - to stop it acting otherwise, going elsewhere, or successfully stabilizing its own alternative version of technological and social relations." (1992: 9) This stabilization of a particular technology puts an end to the various interpretations that can be placed upon it and the practices that surround it. The potential for such interpretation seems greatest in the earliest days of the technology's development. The fact that opportunities exist for alternative views of technological use

is referred to as 'interpretative flexibility'; the gradual whittling away of such opportunities is termed **closure**. Bijker and Law describe how:

> Technologies and technological practices are built in a process of social construction and negotiation, a process often seen as driven by the social interests of the participants. Closure is then defined as, "the process by which conflicting groups reach (or impose) a specific outcome and so conclude the dispute" (1992: 13).

The question arises as to when, if at all, the ability of social groups to shape a technology is largely eliminated because the technology has assumed innate characteristics: that is, it is said to have a 'trajectory'. To some extent the history of hacking will be shown to verify such a scenario. The earliest hackers followed the 'hands-on imperative' and were actively involved in the programming and hardware modifications of the very first computers. The most recent generation[1] of hackers, have been stigmatised to the extent that they are now the subject of criminal legislation, and thus have a very limited role in the formal development of computing. Thus computing has arguably been subjected to some degree of 'stabilisation' or 'closure', the alternative conceptions hackers might have of computing having been largely marginalised. The study portrays the processes by which this marginalisation and stabilisation occur. This said, the recent court case involving the young hacker Paul Bedworth[2] has produced doubt as to whether computing has experienced unequivocal closure. The seeming inconsistency of some juries in such cases of computer misuse seem to suggest that computing is involved in an on-going and unresolved process of change and negotiation. The thesis as a

---

[1] A full account of the different generations of hackers is contained in Appendix 2.

[2] On March 17th 1993 he was charged under the 1990 Computer Misuse Act and acquitted, yet in the same case, two other hackers were convicted on 21st May 1993, for what the judge described as 'intellectual joyriding'.

whole, therefore, seeks to question whether any alleged process of closure can successfully be exerted against hackers.

1.2 THE SIGNIFICANCE OF HACKING

A study of hackers has particular theoretical significance for social shaping theories because they are an example of a non-dominant group influencing a very powerful area of technology: a phenomenon largely ignored by such theories. Molina, for example, makes the assumption that "the influence of non-dominant social forces is taken as subsumed in the practical decisions and actions of the dominant social interests" (Molina 1989: 3). In contrast, this study describes how the actions of the the dominant social groups within computing, rather than subsuming the CU, are often in fact formed as responses to it. A dramatic example of this is the way in which the very nature and identity of the CSI results from the differentiations it actively seeks to make between itself and the CU: a deliberately engineered scenario of 'them and us'.

More generally, hacking is an inherently interesting area to research. Computers are arguably modernity's most important technological artefact as society is increasingly being structured around various networks of interrelated technological systems that are ultimately linked and coordinated by means of computers. The growing interdependence of systems has increased the profile of hackers by raising their potential to cause harm or inconvenience.

The original clumsy valve-based machines have been replaced with hugely more efficient silicon chip-based models, and this has produced an equally substantive evolution in the nature of information. It is now much easier to produce and communicate information and its increasing importance is continually emphasised by such commonly used terms as "Information Technology" (IT) and "The Information Revolution". The rapid proliferation of computer-generated information has also heightened the public profile of hackers. The study was begun in 1989 just when hacking was starting to be a news topic of interest to the general public. Despite

the fact that the origins of hacking have been traced to the MIT computer labs of the late 1950's, general public ignorance of hacking has prevailed, until recently. In 1990 the Computer Misuse Act was passed in Parliament making computer hacking a criminal offence, and hacking was topical enough to be included in the plot of the Australian Soap-Opera Neighbours and such feature films as War Games, Sneakers, and most recently in Jurassic Park the antics of an 'evil hacker' (who fulfills the stereotypical hacker image down to his dependence upon junk-food and his immature personality) contribute to the breakdown of the dinosaur-park's security measures.

A third element of hacking that has made it increasingly interesting to the public is the combination of its particular technological content with the human element of its ingenuity and daring[3]. The close relationship of cunning and technological guile is a perennial area of interest for human beings:

> In ancient Greece, children learned the value of cunning from the exploits of Odysseus, the man 'of many devices'. American Indian children learned cleverness from the mythic figure of Coyote the Trickster. All folklore features these masters of guile, who teach that a good trick may outdo the strongest sinews in the risky adventures of life. In the modern West, the survival power of the mind has come to be concentrated in the 'many devices' of our technology, and now most importantly in a smart machine which is the culmination of that technology (Roszak 1986: 66).

It is common for the public to view computers with the often closely related emotions of fear and awe. Computers are feared because they contain large elements of the unknown 'big black box' that characterises the technology prevalent in a society where few

---

[3]In an article from the New York Times (20th April '91) Erdwin Pfuhl, a professor of criminal law at Arizona State University, describes as the 'Rust-effect' the tendency of the public to be interested in hacking. Rust is the name of the West German 'sports flyer' who broke through Soviet Air defences and performed a 'fly-by' of the Kremlin.

people have technical knowledge. This ignorance of computing may also quickly translate into awe at the results computers can produce. Hackers are thus of immediate interest because they are simultaneously adept at utilising computing facilities and at subverting the security and purposes of the technology they use. They exhibit both knowledge and daring with respect to the computers that people often fear to the point of irrationality[4]. The fact that large computer systems also tend to be owned by large organisations lends to hackers an added quality of providing vicarious revenge to the 'average people in the street' over the faceless bureaucracies that are normally perceived as oppressing them.

1.3 RESEARCH QUESTIONS

(i) Hackers and technological determinism.

The phenomenon of hacking raises questions as to the nature of the process by which certain social groups gain control over technology. Social shaping theories debunk the more simplistic aspects of technologically deterministic theories by giving evidence of groups that shape technology to their own requirements. A weakness of such theories, however, is that they tend to concentrate only upon those groups influencing technology that are part of a dominant social interest group. Hackers threaten such notions by influencing computing as a non-establishment sub-culture, hence their soubriquet 'the computer underground'.

(ii) Hackers' counter-culture status

The thesis describes the nature of the beliefs and motivations that set hackers apart from other groups within computing. From

---

[4] Beqaui (1987) gives such examples as the Californian Highway Patrolwayman who feeling threatened and frustrated by his computer, shot it. There are also anecdotes of people believing that they could catch a computer virus fom the keyboard of their computers.

this description arises the question of whether hackers can be identified as a particularly cohesive group. The research addresses how the CU contains disparate factions and the extent to which it is unified as a community in its opposition to various ideological positions of the dominant groups within computing. Added complexity arises from the fact that there are 'internal' and 'external' perceptions of what it is to be a hacker. The CSI have different perceptions of what constitutes a hacker than the hackers themselves. For example, the latter distance themselves from the propagators of viruses, whilst the CSI tend to group the two together. The research aims to answer the question of how these different perceptions are reflected in the values and ethics people hold within computing and, in turn, how these ethics influence their computing activities.

(iii) Boundary formation

In the early MIT days of computing hackers existed within the main body of computer users. Computing's development, however, has led to the emergence of separate groupings within computing and, in particular, in the polarisation between the CU and the CSI. The research questions the solidity of these boundaries between groups. Both the literature and fieldwork illustrate how the 'Balkanisation' of computing into these groups has proceeded problematically.

Hackers and their 'adversaries' in computer security are both part of a new environment in which knowledge about security weaknesses is at a premium. Despite the need for improved system security, the state of computing is such that there is no official Academy of Hacking or Computer Security Protection Agency from which standardised and recognisable qualifications can be obtained. Evidence is examined of the way in which the technical knowledge hackers possess is being ignored for non-technical reasons. Questions are asked as to why this is so, and what the significance is of the decreasing tendency for hackers to move into jobs relating to the

provision of security. The study shows that although the constituency of computing is amorphous and therefore often missing an easily identifiable structure, group identity is crystallizing as the mobility between groups slows down.

(iv) Stigmatisation

Leading on from questions concerning the stability of the boundaries between groups is an associated issue of whether there is still an active role for hackers to play within computing, or whether they have been largely excluded from any active part in its future development. Hackers have been marginalised and stigmatised as part of the boundary formation process. They have been portrayed on the one hand, as 'technological wizards' and as 'surfers on a technological wave'[5] whilst, on the other hand, media portrayals of hackers emphasise their purported malice and 'dark' motives. The study traces this process of stigmatisation by describing the 'them and us' moral positions increasingly articulated by the nascent CSI; the way in which physical analogies are used to emphasise these positions; and the process's most obvious manifestation - the legislation that has made hacking a criminal offence.

(v) Policy Issues

The thesis concludes by asking what the implications of such legislation will be for both the future of hacking, and computing as a whole. With respect to the 1990 Computer Misuse Act, the study asks which policies are the most liable to reduce hacking and whether criminalising it is likely to solve the problem or risk pushing it further towards the conventional criminal underground.

1.4 SCOPE OF THE STUDY

---

[5]Jacques Vallee (1984)

The study aims at filling gaps that exists in academic coverage of the issue of hacking. Most of the coverage is media-based with journalists being the main authors of the existing literature. This study adopts a more theoretical and less biographical approach to hackers and their activity. The most recent entrants identified in the study have born the brunt of the anti-hacking legislation passed during the course of the research which made it difficult to gain access to currently active hackers. This problem was offset by concentrating upon older, more established, sometimes retired hackers, and by broadening the scope of the study to protray external perceptions of hacking as voiced by the other main groups within computing. The youngest hackers are therefore not part of the first-hand focus of the study. Brief discussion of their significance stems from the evidence of the older hackers and is largely left for future research.

A deliberate ommission is the study's concentration upon the more narrowly-defined activity of hacking in contrast to the broader definition of computer crime which includes virus-writing and fraud. The rationale for avoiding these activities is that they are more obviously traditional crimes that happen to be using a computer as a means to their illegal end, rather than an end in itself. They are manifestations of the traditional crimes of vandalism and deceit for personal gain, albeit in a new technological guise. They do not pose theoretical questions of the same level of interest as non-malicious hacking.

1.5 OUTLINE OF CHAPTERS

To summarise the account of computing presented in this study: Chapters 1-4 introduce and explain the nature of hacking, and place it within a wider context of technological change as a whole. This first section of the thesis introduces the evolution of information and how this has resulted in new ethical questions being raised regarding the ownership of and access to information. The second section of the thesis, Chapters 5-7 portrays the competing ethical

outlooks of the Computer Underground (CU) and the Computer Security Industry (CSI) which give rise to the process of attempted stabilisation or closure: a main theme of the thesis.

Chapter 2 - Methodolodgy

This chapter describes the research methodology employed in this study and how it was adapted to include electronic mail correspondence and interviewing techniques. The various advantages and disadvantages of electronic mail as a methodological tool are discussed.

Chapter 3 - Hackers: the evolution of information and technological change

Chapter 3 examines the extent to which hackers illustrate various themes from social theories of technological change. It starts by examining the notion of technological determinism and proceeds to analyse how hackers simultaneously embody its concerns, and yet also provide a prime example of a societal group involved in a process of actively changing the technology of computing, through its interactions with other groups and its influence upon the artefacts themselves.

Theories of technical change that emphasise this social shaping element are examined, focusing upon the locus of power within such a process. The potential power hackers may have to influence computing is questioned in terms of its viability as a culture embodying alternative ideals to the dominant social group's, and the likelihood of such ideals being translated into a coherent programme of political change.

The programme of change intimated in the first part of Chapter 3 rests upon hackers' alternative interpretations of the political and economic qualities of information. This chapter explores these interpretations showing how hackers oppose increasing market pressures to commodify information. The role of hackers in

questioning conventional notions of information is further examined in a section dealing with the informational concept of 'cyberspace'. Descriptions are given of the qualitatively new situations that arise because of information's increasing tendency to assume immaterial forms. This description of the most recent and dramatic stage in the evolution of information lays the basis for the study's subsequent coverage of the ethical debate between the CSI and the CU.

Chapter 4 - Hacking: culture and motivation

The purpose of Chapter 4 is to describe how the literature portrays what it is to hack, and the nature of the hacking community, consolidating and extending this portrayal with material from the fieldwork that compensates for lacunae in the literature's coverage. The resultant survey of the main features of hacking and its environment forms the basis of the empirical examination in subsequent chapters of hackers' social role in the technical development of computing.

The chapter takes the form of a presentation of what hackers percieve the Computer Underground (CU) to be. It is based on descriptions by hackers of their activity, both from the study's empirical interviews and from literature in the field. The basic elements of 'the hack' and 'the hacker ethic' are portrayed as an introduction to more specific aspects of the culture of hacking. Hacking culture is found to be characterised by its heavy reliance upon technological artefacts; by interactions based on anonymity and secrecy; by amorphous and fluid relations with the rest of computing; and by the fact that it is an overwhelmingly male culture.

The second part of the chapter focuses upon the specific reasons why hackers feel the need to hack. A full rationale is first given for largely excluding certain activities such as virus-writing from the analysis. Thereafter, extant academic analyses of hacking are introduced but criticised for their lack of breadth. A more detailed and comprehensive examination of the motivations for

hacking follows that is based upon hackers own descriptions of why they hack.

Chapter 5 - State of the Industry and the Computer Security Industry (CSI)

This chapter concludes the portrayal of the main groups within computing, the wider theoretical significance of which will then be analysed in the remaining chapters. It describes the two major branches of the CSI: the 'hawks' and the 'doves', so named for their differing approaches to the question of potential cooperation with hackers. The two views are compared and contrasted, introducing the reasons for and against making use of the technical knowledge hackers have of systems as a means of improving their security.

The relative ease with which hackers obtain access to other people's systems is described, which illustrates that there are severe and widespread security faults. The chapter also looks in detail at the nature and scope of security weaknesses within computing. The statistics produced by the National Audit Commission and the National Computing Centre's reports on computer crime, along with the data gathered from the study's quantitative questionnaire are examined. The extent of these faults is explained in terms of poor levels of knowledge and education about security issues.

That hackers can make use of security faults to gain unauthorised access implies that they have information that is useful to those wishing to improve the security of systems. This potential is explored with an analysis of the specific arguments that contend hacking has a potentially useful technical purpose. The question then arises as to why there seems to be little cooperation between hackers with knowledge of security gaps, and those wishing to improve the security of systems. This is described in the subsequent chapters as being due to a process of closure whereby hackers are deliberately excluded from having an influence in the development of computing.

Chapter 6 - Ethics and Stigmatisation: "them and us"

The chapter introduces the whole issue of ethics within computing vis- á -vis hacking activities. It describes the vestigial and often blurred nature of such ethics which is due to the emerging status of the CSI and the relatively new phenomenon of hacking (at least in a widespread form). Specific examples from discussions within the CSI of such ethical ambiguity are given along with some of the technical reasons for the ambiguity.

The maintenance of a gap between the CSI and hackers can be seen as part of a group formation process whereby the emerging CSI is creating an identity defined by its opposition to the CU. The chapter looks at various examples of this boundary defining process with reference to the activities of computer professionals and interest groups, both from literature sources and fieldwork interviews.

Analysis of the ethical questions surrounding hacking is extended in this chapter by a discussion of the role of analogies in the debate between the CSI and the CU. Analogies are shown to be utilised predominantly by the CSI as part of a boundary formation exercise that distances itself from the CU, whilst at the same time, serving the purpose of establishing and reinforcing its own identity. Attention is drawn to the inherent weaknesses associated with the use of physical analogies, giving the specific illustration of the comparison made between hackers and the cowboys of the Wild West.

Chapter 7 - Criminality

Chapter 6 illustrates some of the pressures that have led to a legislative response to hacking. This chapter furthers that analysis by specifically addressing the implications and consequences of the debate that accompanied the parliamentary passage of the Computer Misuse Act. The chapter refers to the "disembodied" nature of computer crime; the various specific purposes of the legislation; and

the likelihood of the legislation achieving its stated objectives. The possibility that hacking legislation may, in some respects, be merely a symbolic response is also considered. Illegal computer activity is described (in so far as the fieldwork could produce evidence of criminality in the face of obvious disclosure problems). Finally, the practical consequences of exposing hackers to the prison system are briefly explored.

Chapter 8 - Conclusion

The final chapter summarises the contribution of this work to existing literature about hacking and comments upon its novel methodological utilisation of e-mail techniques. The process of stigmatisation described throughout the body of the study is assessed in relation to its implications for policies aimed at reducing the incidence of hacking. The chapter also pays particular attention to the study's comparison of the account of hacking given by hackers themselves (the internalist account), and the different interpretation of the activity made by outsiders (the externalist account).

Chapter 2 - Methodology

2.1 INTRODUCTION

2.2 CHOICE OF RESEARCH METHODS AND INSTRUMENTS

2.3 ADVANTAGES AND DISADVANTAGES OF E-MAIL AS A METHODOLOGICAL TOOL

2.3.1 Advantages

2.3.2 Disadvantages

2.4 SPECIFIC E-MAILING TECHNIQUES

2.5 CONCLUSION

2.1 INTRODUCTION

Various methodological problems arose in this study's analysis of the phenomenon of hacking. The most obvious of these relates to the fact that, by its very nature, computer-based communities are not such an easily identifiable social group as their 'real-world' counterparts. The disadvantage posed by this lack of physicality is that the researcher does not have a group of people with institutionalised degrees of seniority and knowledgeability with whom they can converse.

At an early stage of the thesis it was realised that conventional assessments of expertise were not appropriate for the various subject areas of the resarch. In keeping with the frontier and hobby-like aspects of computer security, knowledgeable people were found widely dispersed within the computing community. As a result, empirical data sources for the research came from a wide range of electronic-mail (e-mail) interviews with contributors to various electronic-mail publications[6]. These were supplemented by more traditional face-to-face interviews with figures from the main computing groups and additional interested parties such as spokespersons for the Department of Trade and Industry and the police.

The various methodological tools listed below were used in order to overcome the above problems, and to fulfill the overall aim of this study: to describe the experiences and attitudes of the wider computing community that exists, between and including, the two poles of professional computer security experts and dedicated system crackers. We shall see shortly how boundaries between the various groups within computing appeared to be somewhat amorphous. For example, some individuals had originally become involved in computing through hacking, and are now concerned with

---

[6] Electronic mail publications are magazine digests that are published in electronic form and then either archived and accessed by those wishing to read them, or alternatively, sent out on an automatic mailing list to those who subscribe (generally at no cost).

the preventative side of computer security, either in their work as security consultants, or, alternatively, as computing officers in charge of the maintenance and development of academic systems. Thus the rationale behind using the methodological tools described in this chapter was to achieve a broad cross-section of the opinions and experiences of the net community from which a more representative and realistic account of hacking and its implications could be derived than would be possible with a more compartmentalised approach.

Meyer (1989) in his study of hacking culture, cites three basic approaches that could be utilised in investigating hackers as a "deviant group". These are:

1. social psychological: looking at the motivations and personal characteristics of hackers.
2. socio-structural: - addressing the implications of hackers for society.
3. social organisation of deviant groups: analysing the way in which hackers structure their relations amongst themselves.

In contrast to Meyer's preference for the third of these approaches, this study prefers to combine elements of both 1 and 2, analysing them more fully than has hitherto been attempted. This is done by building upon the 'internalist' description of hacking given by hackers themselves, and supplementing it with the 'externalist' account from their opponents. The study thus includes the opinions and experiences of diverse figures in the computing community, describing the interactions of hackers with other groups within computing: an external as well as an internal account.

2.2 Choice of Research Methods and Instruments

(i) Interviews

A series of semi-structured interviews were conducted: they were either traditional face-to-face interviews, or based upon e-mail

correspondence over a prolonged period of time. During the research, e-mail-based interviews assumed an increasingly significant role in the gathering of empirical data. Face-to-face interviews were largely used as a means of initial research design, and in order to engage with key figures identified as being poorly represented by the e-mail method.

Variations on the semi-structured e-mail interviews included two interviews with figures from the USA: Prof Spafford from Purdue Technical University sent me an audio tape of his thoughts to specific questions I had e-mailed to him, in order to supplement our correspondence. Another, particularly inventive, interview was conducted with an American hacker, who, because of the conditions of probation that he was under, was not allowed access to computers and hence was unable to take part in an e-mail dialogue. The interview took place by a phreaked phone[7] call from the hacker and was recorded directly from the phone at my end of the call.

(ii) Method of contact

The UK based face-to-face interviews were obtained in the orthodox manner of writing to those perceived to be key figures within computer security. These perceptions were influenced by a combination of their professional occupation and reputation, along with their reputation amongst the computing circles actively using e-mail, and contributing to electronic magazines. The Dutch-based face-to-face interviews initially stemmed from two e-mail contacts from which further contacts 'snowballed'. The empirical data gathered in the Netherlands proved particularly useful. At the time of the research starting, British hackers seemed to have largely disappeared from public (electronic view) as a result of the passing of the Computer Misuse Act in 1990; in contrast, Dutch hackers at this time, enjoyed general freedom from hacking-related prosecutions. In addition, contact with Dutch hackers proved useful

[7] A small prototype touch-tone dialler was used which was capable of obtaining unbilled long-distance phone connections.

as means of gaining further access to their hacker associates in several countries because it provided me with a firsthand opportunity to prove my non-establishment credentials (in so far as my interest in their activities was purely academic) and thus gain their trust and help in meeting more hackers. Sole reliance upon e-mail interviewing would have made breaking the initial barriers of suspicion much more difficult.

An imaginative approach had to be used for making contact with hackers reluctant to risk possible incrimination under the Computer Misuse Act which was passed halfway through this piece of research (1990). In addition, it became apparent at an early stage of the research that a disproportionate amount of time could be spent on the ultimately impractical aim of seeking subjects fully representative of an indeterminate and mercurial culture. One example of the generally ad hoc and unorganised nature of the computer underground was my request to one of my e-mail correspondents, John Draper, to pass my e-mail address to hackers present at an annual underground 'conference'. His response illustrates the anarchic structure of underground groups and the subsequent difficulties encountered in attempting to gather information even in environments full of hackers:

> I tried to contact them, but the HoHoCon[8] situation was such that it was almost impossible to find any one individual, as there was no common place where people can meet. All meetings were done in hotel rooms, and there was no list of rooms, and the only way to do that was to stay outside and grab people going from room to room (Draper: e-mail interview).

Weariness of press contact and language problems also seemed to exclude the relatively active German hacking scene which includes such organisations as The Chaos Computer Club of Hamburg, whom I made several unsuccessful attempts to contact.

---

[8] This was the name of the conference.

The contact that was made with e-mail correspondents resulted from spending relatively large amounts of time reading various electronic magazines and newsgroups, and forwarding a list of e-mail questions relating to various hacking issues which was posted widely around the internet. From a large number of responses (90-100) to this questionnaire, the main areas of interest common to both myself and the respondents became clear. It also became clear, from the length and amount of detail given in the responses, who was most likely to be informative to the research. These respondents were then targeted for a more concise list of questions based closely upon their original response, and in this manner an electronic dialogue was entered upon with various individuals which, in some cases, lasted several months.

(iii) Sampling and Representativeness

The respondents were self-selecting to the extent that they all had access to the internet and regularly read and/or contributed to the newsgroups. This led to an original bias in the list of responses to people from academia and US citizens. The latter bias was inevitable due to the predominance of US users on the internet and the lack of realistic alternative means of communication, but it was off-set somewhat, by the european-based nature of the fieldwork. The academic bias was countered by using an e-mail directory from the commercial sector, and dispersing the questionnaire amongst as many commercial sites as possible.

The willingness of hackers to chat with me had the implied disadvantage that they were unlikely to be actively involved in clandestine hacking activity. The general consensus of opinion from those that would talk was that active hackers tended to lie low due to the fear of prosecution stemming from the CU's recent experience of various law-enforcement 'stings' or undercover operations. Those that were contacted consisted of mostly 'retired' hackers, who, through a lack of current activity, felt more at ease discussing hacking issues. Also, some of the garruloussness of hackers

interviewed seemed to be due to the fact they had already been investigated by the Secret Service or experienced prison[9], and therefore were more aware of what they could safely confide to me, these interviewees lacked the general feeling of concern and suspicion that seemed to inhibit others in the net community.

The extent to which my e-mail respondents were representative of the computing community as a whole is dependent on the fact that they use e-mail in the first place and, furthermore, that they tend to be the most regular and voluminous of contributors to the various electronic magazines that formed the basis of my sampling area. The first of these potential objections is insubstantial given the fact that an almost intrinsic prerequisite to membership of the international computing community is a tendency to use e-mail. The second limitation was justified on the basis that those willing to spend large amounts of time making such contributions would also be more likely to engage in time-consuming correspondence with me.

2.3 ADVANTAGES AND DISADVANTAGES OF E-MAIL AS A METHODOLOGICAL TOOL

2.3.1 Advantages

(i) Costs and space

The low-cost and university-funded nature of much e-mail correspondence resulted in it becoming an extremely useful information-gathering instrument, in a subject area where the geographical spread of subjects would have made more traditional forms of interviewing prohibitively expensive.

(ii) Speed and interactive nature

---

[9] As in the cases of Eric Coggans (Legion of Doom) and John Draper (Captain Crunch), respectively.

Once an interesting avenue of research had been identified from an electronic response, greater expansion or clarification could be more easily and effectively sought than would have been possible compared with a normal face-to-face interview, which tends to be of the 'once and for all' form of information extraction. The possibility of practically interactive clarifications of key research issues soon became apparent, largely as the serendipitous result of the study's progress. This said, the methodological implications of e-mail are ambivalent to the extent that it allows the respondent more of a chance to reflect upon issues, and so to refine their responses. This may increase the accuracy of replies, but it may also reduce some of their spontaneity.

(iii) Increased response rate.

A pleasant surprise from the fieldwork came from the amount of 'high profile' actors in the field of computer security who were prepared to spend considerable amounts of time corresponding by e-mail. Apart from the obvious geographical problems I would have encountered attempting to interview the main actors in the area of computer security, it is debatable whether I would have been accommodated so generously into the schedules by some of the main figures in this study. An aspect of e-mail which may facilitate this apparently greater willingness to communicate than by face-to-face or phone methods, is the fact that e-mail, although almost instantaneous when required, can otherwise be answered when the recipient chooses. This creates the impression that e-mail correspondence is less burdensome, even though, judging by the detail of their replies, for some of my respondents, their replies were obviously very time-consuming. The ease with which e-mail is transmitted can lead to bothersome back-logs just as with the paper variety of message. Arguably, however, e-mail backlogs are not as off-putting as a heaped 'in-tray', and furthermore, the 'reply' function of e-mail programs reduces the time needed to deal with an

e-mail enquiry by automatically sending any typed response to the destination of the original message.

2.3.2 Disadvantages

(i) Absence of regulating feedback

Due to the 'disembodied' nature of e-mail communication, no visual or aural cues can be used with which to intimate the limits required for the response to a particular question. On occasion this reduced the efficacy of correspondence, as the particular nuances and thrust of a question may be overlooked, and a second corrective number of questions may need to be sent.

(ii) Validity

Again due to the 'disembodied' nature of e-mail it can be difficult to verify the veracity of the respondent's identity, and the content of their responses. The study's Dutch fieldwork, however, involved face-to-face interviews with previous e-mail correspondents and they seemed to validate e-mail as a legitimate method of interviewing.

2.4 Specific E-mailing techniques

In addition to the above methodological aspects, specific ad hoc techniques were used as some of the idiosyncracies of e-mail interviewing became more apparent. Examples of this include:

(i) Mailing list targeting.

This technique refers to the use of an electronic mail address register for approximately 400 British commercial sites from which just under 40 responses were gathered in a single mail shot. The 10 per cent return rate was achieved with a 'cold' targeting technique

(the questionnaire was sent out to a previously unknown list of contacts with an attached explanatory and confirmatory note from my supervisor). This technique made use of the automatic mail-sending ability of e-mail, whereby a standardised message could be simultaneously sent out to all commerical sites on the list.

(ii) Personalised Correspondence

Whilst the previous technique proved useful for the standardised distribution of a small quantifiable questionnaire, a deliberate decision was made to avoid using similar techniques with more qualitative questionnaires although, at least in the first stages of the distribution process, automated and standardised methods could have been used. The rationale for this was the belief that the response rate of more discussion-based questions would diminish if e-mail messages were received which seemed to be of a standard, depersonalised format. Thus, although the first batch of broadly focused qualitative questions were sent out to individual respondents from a stored file, a personalised, explanatory and introductory message was sent with each list of questions. Whilst there is no conclusive way of establishing whether such an approach did in fact increase the response rate, it did serve to establish an early rapport with some respondents, evidence of which being the friendly, light-hearted tone of many messages. This emphasises the electronic medium's apparent predisposition to produce solicitiously helpful and readily communicative correspondents. It is also likely that such a rapport subsequently facilitated my efforts of 'snowballing' existing respondents so that they gave me some access to their network of colleagues or 'net-friends'. The best example of this was the extended fieldwork I conducted in the Netherlands from my initial e-mail contact with one Dutch hacker.

2.5 CONCLUSION

To summarise: the research design and methodology were adapted to make the fullest use of the efficiency of e-mail as an information-gathering tool relevant to all sectors of the computing security constituency. The novelty and scope of the research were thus enhanced by e-mail. It allowed access to a hacking culture that would otherwise have been closed to observation from an outside source due to both the desire, catered for by e-mail, to remain anonymous, and also due to the large geographical spread of the computing community.

Chapter 3 - Hackers, theories of technological change and the changing nature of information

3.1 INTRODUCTION

3.2 TECHNOLOGICAL DETERMINISM

3.3. HACKERS AND TECHNOLOGICAL DETERMINISM

3.4 TECHNOLOGICAL POLITICS

3.5 LATOUR AND THE PRINCE
3.5.1 Hackers and the Prince

3.6 THE CHANGING ECONOMIC NATURE OF INFORMATION

3.7 CYBERSPACE - THE REAL AND VIRTUAL WORLDS
3.7.1 Cyberspace and technological domination
3.7.2 Cyborgs: a rejection of technological determinism
3.7.3 Cyberspace and the culture of opposition

3.8 HACKING AS AN ALTERNATIVE CULTURE
3.8.1 Opposition to commodification
3.8.2 Hacking as anti-bureaucratic rebellion
3.8.3 Anti-Government sentiment - privacy and double standards

3.9 CONCLUSION

3.1 INTRODUCTION

The hacker is a figure of ambivalent status in the public's perception. He[10] may symbolise the 'little man' against the big corporations, or equally, the electronic manifestation of the urban mugger. Both of these perceptions derive from deterministic conceptions of technology. People resent the fact that computers are controlled by faceless bureaucracies: hackers can be seen as the 'man in the street's' vicarious revenge over the 'system'. They also, however, fear hackers, they feel vulnerable to the threats posed by the potentially random electronic violence of the sociopathic hacker. Computing is thus perceived as either inevitably oppressive and conducive to Orwellian-type control or, in contrast, beyond control to the extent that it is vulnerable to sabotage and possibly catastrophic breakdown.

This chapter examines the notion of technological determinism, applying it to hacking and the 'information revolution'. Social shaping theories of technological change seek to explain what is referred to as the 'heterogeneity of factors' that influence and shape the development of a technology. Social groups seeking to influence technology in their preferred direction have arrayed against them the dominant social forces that stand to lose power and/or material benefit from such interference. These dominant social forces are variously described as 'the establishment', 'the dominant social constituency', and Latour's (1986) notion of 'the Prince'. This chapter analyses within in the context of such theories the role hackers play in opposing the dominant social constituency's agenda within computing.

The advent of computing has brought conflicting pressures to the way in which information is treated in society. Computers add value to information due to their ability to manipulate it faster than previously possible, whilst simultaneously weakening the properties of information that could be subjected to proprietary claims. It is

---

[10]The male predominance of hackers is described fully in Chapter 4.

upon these claims that the commodity status of information ultimately rests. Quantitative improvements in the processing of information have become so fundamental as to threaten changes in the qualitative nature of information: changes that challenge information's status as an economic commodity. There is a growing tendency for the barriers of exclusion upon which information's commodity status depends to be weakened. The barriers are becoming less and less material in form as its means of diffusion become more diverse and productive, and this is reflected in the behaviour and attitudes of consumers who increasingly fail to respect informational copyright in areas as diverse as computer software and pop-music recordings. There is thus an immediate source of conflict between those seeking to exploit what they perceive to be the weakening of information's commodity properties and those seeking, in contrast, to enforce its property rights.

The relationship of hackers to information provides a vivid example of one side of this conflict: they pay scant respect to conventional notions of property rights. Evidence of hacking's oppositional status is presented, in two particular areas: software copyright and system intrusions. In the former, proprietary claims are eschewed in preference to those elements of information conducive to widespread sharing and duplication. In the latter area, hackers perceive traditional notions of privacy as inapplicable in many computer-based situations. Their unwillingness to be affected by considerations of other peoples' privacy is fuelled by the alleged invasions of privacy either routinely carried out by the establishment, or allowed to continue as a result of its perceived negligence in failing to improve the security of the computer systems under its control. Hackers subsequent interpretation of information and its place in society is markedly different to that of the dominant social constituency. It is most evident in the notion of cyberspace which provides a framework with which to explore their claim to be an alternative culture. The 'cyberpunk' genre of science fiction describes hackers mentally travelling through lattice-like structures of information known as cyberspace or the matrix. The usefulness of

this fictional account as a portrayal of hacking culture's anti-establishment nature will be analysed.

3.2 TECHNOLOGICAL DETERMINISM

The perennial subject of technological determinism is of special contemporary significance with regards to the widely imputed phenomenon known as the 'information revolution'. Technological determinism is in its crudest form, "the idea that technology as the sole result of an internal dynamic, and then, unmediated by another influence, moulds society to fit its patterns" (Mackenzie and Wajcman [eds] 1985: 26). The concept can be split into two major areas, namely, technological determinism seen as, either, a uniformity of impact on society, or, as technology having an autonomous realm of its own. In addition, it can also be viewed as the powerlessness of humans faced with the speed of technological change; speed such that social structures are forced to adapt to technology rather than vice versa. The notion is that there is a 'cultural lag', as society attempts to catch up with the technological changes it is undergoing.

The fundamental fear associated with the notion of technological determinism is that technology is out of human control. It is compounded by doubts as to whether, even when human beings have nominal control of technology, it is invariably used for destructive purposes. Lorenz argues that such behaviour can be traced back to homo sapiens at the earliest stages of its development:

> Obviously instinctive behaviour mechanisms failed to cope with the new circumstances which culture unavoidably produced even at its very dawn. There is evidence that the first inventors of pebble tools, the African Australopithecines, promptly used their new weapons to kill not only game, but fellow members of their species as well. Peking Man, the Prometheus who learned to preserve fire, used it to roast his brothers: beside the first traces of the regular use of fire lie the mutilated and roasted bones of Sinanthropus Pekinenis [Peking Man] himself (Koestler 1987:339).

The relationship between humans and technology is thus seen as an uneasy one. The stark conclusion is that: "The Promethean myth has acquired an ugly twist: the giant reaching out to steal lightning from the Gods is insane" (*ibid*:331). A frequent theme of modernity highlighted by theorists is that of human subordination to technology. A series of thinkers have emphasised a loss of human control in the face of technology which seems to have created its own independent path or trajectory of development. Martin Heidegger, for example, anthropomorphises technology and highlights the inevitability and finality of a process out of man's control (Winner 1971: 14). Computer technology has dramatically increased these fears. Hackers are an example of a group, the health of whose relationship with technology has been questioned and yet who offer the potential to break away from the sort of technological domination Heidegger describes.

3.3 HACKERS AND TECHNOLOGICAL DETERMINISM

In the theoretical literature there are ambivalent views as to what hackers signify in the process of technological change. Hackers are viewed as either a reassuring element of humaneness in the otherwise dehumanised realm of technology; alternatively, they are seen as a startling example of the degeneration of human values within technology. Using a mythological analogy, Michael Shallis (1984) argues that the above defence of hackers is untenable. He points out that these feelings of powerlessness and the concomitant relationship between human beings and technology can be usefully described as a modern form of the myth of Narcissus. He argues that technology produces an insiduously numbing effect, the most extreme example is that of the hacker: Narcissus being his

mythological representation. The argument is that groups such as hackers and their addiction to the technology of computers merely illustrate the wider phenomenon of man (sic): "becoming a servo-mechanism of the technology, adapting to the technique and becoming thereby closed to the world. Such a procedure ... manifests itself in the notion of the technological imperative: the idea that technology has a life of its own, what can be done must be done. It is the argument of a Narcissus treating his own reflection as an end in itself" (Shallis 1984: 80).

This study looks at how hackers fit into a scenario outlined by writers such as Marcuse (1964) and Shallis (1984), who see human beings increasingly finding themselves in a symbiotic relationship with the artefacts of technology. Shallis argues that people and technology tend to form a feedback loop or servo-mechanism. He points to the idea that the demarcation line between human identity and the artefacts created by it is increasingly blurred. The image of Narcissus appears again with Latour's conceptualisation of the appropriate methodology with which to approach the analysis of technology. In a seminar at Edinburgh University[11], he finished his talk by arguing that the general interpretation given to Mary Shelley's Frankenstein was symptomatic of the general myopia with which the area of technology is usually approached. Her novel is most often interpreted as an account of how man tends to lose control of his creations. Latour argued that it would be more productive to see the novel in terms of a love story. Frankenstein failed to love his creation and it is this rather than any inherent uncontrollability of the invention that was the reason for the story's tragic dénouement. If Latour is correct and the most important element of technological change is not the characteristics of the artefacts we produce, but rather the way in which we relate to them, then the case of hackers is an intriguing area of investigation. Hackers more than any other group involved with technology epitomise what it is to love a technology, it remains to be seen

---

[11] Summer 1990.

whether this love is the Narcissistic love of the technological imperative or whether in fact hackers are an example of a group that are pioneers in the field of producing non-alienating human-technology relationships.

In deterministic theories of technological change hackers are seen as an illustration of a trend within society: the denigration of human reason and its subordination to 'the cult of information.' In this general context of technological confusion and anomie, hackers are portrayed as having gained mastery of their chosen technology yet at the cost of having lost some of their humanity in some sort of Faustian bargain. In One Dimensional Man Marcuse talks in terms of modern man only finding his soul in his hi-fi, split-level cooker, or any other modern consumer durable. Similarly, Weizenbaum describes hackers as obsessed and addictive, almost manic, their behaviour leads him to even argue that, "I'm coming close to believing that the computer is inherently anti-human - an invention of the devil" (1976: 125).

The study examines whether hackers can shed light upon the pessimism or realism of such a sentiment at both the level of their individual relationship with technology and to the extent that their activities are conducted in a societal context. In contrast to the pessimism of technologically deterministic theories, hackers represent a positive aspect of human interaction with technology. For example, the increasingly immaterial nature of information has led to new perceptions of what it is to use or 'relate with' a computer. Computers have arguably produced qualitatively new human experiences. Hackers in the sense of compulsive programmers claim to experience mind-machine 'melds', they conceptualise their relationship with their computer as involving journeys along the imagined lattice-like matrices of the computer's memory passages. In an ironic reversal of Ivan Ilyich's call for humans to make and search for 'convivial tools' which are embodiments of a 'simple and wholesome' interaction of people and their natural environment, hackers have instead found conviviality with one of the most complex artefacts human beings have produced to date. Jacques

Vallee (1984) describes such a process with relation to a hacker called Chip Tango: "He never speaks of 'using a machine' or 'running a program'. He leaves those expressions to those engineers of the old school. Instead, he will say that he 'attaches his consciousness' to a particular process. He butterflies his way across the net, picking up a link here, an open socket there" (Vallee 1984: 136).

In contrast to the common perception of feeling swamped by technology, hackers like Chip Tango represent a group whose raison d'être is derived from their mastery of technology. Society's reaction tends to produce a mystery and mythology surrounding hackers. They are often perceived and portrayed in the media and the popular mind as computer whiz-kids or even wizards[12]. This portrayal perhaps received its highest profile in the film "WarGames". The film told the story of a young boy who through his computer prowess and hacking skills stopped the Pentagon's central computer in charge of nuclear weapons from autonomously initiating a nuclear exchange with the then Soviet Union. The film's portrayal of hacking combined fear of autonomous technology with the mythical powers of the **young,** technologically competent adolescent. Age, rather than being viewed as conferring the benefits of experience, is portrayed as almost being a barrier to the intuitive grasp of technology that hackers seem to enjoy.

From a societal perspective, the 'cultural-lag' thesis of technological determinism is perhaps the most pertinent to the particular case of hacking. Hackers can be seen as a post-modernist reaction against 'cultural modernity' and its technologically imposed uniformity, they are: "a conscious resistance to the domination of but not the fact of technological encroachment into all realms of our social existence" (Meyer and Thomas June 1989 a:7).

---

[12]A full analysis of this is the subject of chapter 6.

3.4 TECHNOLOGICAL POLITICS

> *technology is most productive when its ultimate range of results is neither foreseen nor controlled* (Winner 1971: 98).

Winner calls for a development of a theory of 'technological politics' with which to make sense of the growing complexity of technology. Molina (1989), in contrast, calls for a new social constituency in the area of IT. He argues that, "it seems that to exploit this new wealth for the benefit of mankind and realise the 'era of computational plenty' for all nations, more will be needed than simply further technical advances. Ultimately, the social framework nurturing the technological revolution may need profound changes" (Molina 1989: 146). It is common for theorists in the field of technological politics to look for the major groups involved in making changes in the social framework. Molina talks of the marginal effects of groups attempting to influence technology in what he sees as a more humane direction, for example, the Lucas Aerospace technology group. He concludes that, "In the present context, perhaps the greatest contribution of these efforts lies in the creation of a valuable technical stock offering potential for a world of different and humane possibilities. From this angle, they show that there is nothing inevitable about the shape of microtechnology and, indeed, the general development of technical systems" (1989:147).

However, for profound changes to occur requires, according to Molina, the setting up of a dominant social constituency. The existence of marginal groups is likely to remain just marginal when in IT the dominant social constituency is as dominant as capital. To reorientate IT away from the trends currently imposed by capital, an alternative social constituency is required, one which will displace the present dominant one and at the same time be able to infuse it with humane ideals. The question then becomes:

> Can those ideals acquire the urgency of over-riding interests - which has proved so successful for the present social momentum to the development of technology? And in the

same vein, which social forces embody these humane ideals in their raison d'être in the same manner as capital embodies the purpose of profit-driven accumulation? (1989:163).

Molina comes to the conclusion that with regard to the dominant social constituency of capital: "only its costly inability to succeed has ever exposed the power complex's fundamental lack of humane purposes ... Somehow people must be shocked out of their confidence in the power complex and thus recognise the irrationality of its means and ends" (1989: 165). This 'shock' required to replace the power complex is only ultimately liable to come about as a result of a "catastrophe" which will then make necessary technological developments based upon more humane criteria. He notes that Ellul and Mumford call for "conversions" away from our "technological mentality". The latter describes a need, "to replace the mechanical world picture, and to give to human personality, as the highest known manifestation of life, the precedence it now gives to its machines and computers" (cited in Molina 1989: 173).

Placing hackers within the context of theories of technological change points to them as having the potential to be a group that can play a useful role in building the "valuable technical stock" necessary as at least a starting point for "a world of different and humane possibilities" (even if their actions are insufficient in themselves to threaten the dominant social constituency). Winner views "the pioneers of radical software" as having the potential to form an "alternative emancipatory culture" that can help towards building a "platform for a more humane tomorrow" (Molina 1989: 179). The study will show the extent to which they provide a good example of a group capable of practising Winner's (1971) concept of **epistemological Luddism**, whereby socio-technical systems are dismantled in order to find out the exact nature of the benefits they bring to mankind. A central tenet of hacking behaviour in various forms is the belief that technology of all sorts is to be understood and mastered rather than accepted as the strange machinations of little black boxes. It is this belief which gives hackers a significant place

in the debate over technological determinism. They are intrigued by the nature of systems and gaining control over, and ultimately 'beating' whatever technological system they confront. Vallee neatly sums up the position of hackers, vis á vis technological determinism, when he describes his meeting with, 'Chip Tango' a 'midnight irregular' and archetypal hacker who:

> looks at the future with enthusiasm. His trust in humanity is inexhaustible. He takes for granted that computer technology is out of control, and he wants to ride it like a surfer rides a wave. The opportunities for fouling up the world through computer power are unlimited, but he thinks that people like him are useful agents in establishing a balance, a sense of humaneness and humor ... when presented with a scenario of a world which increasingly uses information in an oppressive Orwellian manner, [he] replied, "I'm not worried for a minute about the future. If the world you describe is going to happen, man, I can fuck it up a lot faster than the world we live in now! (Vallee 1984: pp150-151).

Hackers see the battle-lines already forming between those who are attempting to promote the non-proprietal diffusion of information and access to computing, and those who wish to impose upon computing the control and commodification elements of the capitalist social order in a manner which is oppressive and ripe for opposition. John Perry Barlow and the Electronic Frontier Foundation call for an educational struggle whereby computer users can safeguard some of the informational rights that they claim have been attacked by an establishment not accustomed to the nature of the new IT realm. They wish to avoid "a neo-Luddite resentment of digital technology from which little good can come ... there is a spreading sense of dislocation, and helplessness in the general presence of which no society can expect to remain healthy." (Statement from the EFF: CuD 1.13)

3.5 LATOUR AND 'THE PRINCE'

The CU projects itself as a group which rejects conventional notions of information and its property rights. This rejection is shown in their acts of computer intrusion and in their general cultural milieu which draws inspiration from works which promote an anti-establishment view of technology and information, such as William Gibson's 'Cyberpunk' fiction. Hackers tend to value information as an end in itself and not as an economic commodity. Both the CU and the CSI define themselves, to some extent, in relation to each other. The two related issues of who controls information, and by extension the technology of computing, and the means by which they control it gives rise to a process of boundary formation and mutual shaping. Theories of technological determinism have one thing in common: they presuppose a linear relationship between technology and society with technology being imposed upon society. Social shaping theories are based on a rejection of such linearity: technologies are shaped by a range of heterogenous factors (Bijker and Law 1992: 3).

In investigating theories of technological change, therefore, full weight has to be given to these factors that affect the final shape a technology takes. Technological development is seen as a process of negotiation and conflict between groups vying for influence: "artifacts embody trade-offs and compromises. In particular, they embody social, political, psychological, economic, and professional commitments, skills, prejudices, possibilities, and constraints" (Bijker and Law 1993: 5 and 7).

The relevance of hackers to theories of technological change relates to the process by which they have obtained their underground status. They have been allegedly marginalised within society, thus reducing the impact their expertise might otherwise have had upon the development of computing. From some hackers' perspective it is because of this diminution of their influence that computers are still predominantly perceived as being used in impersonal or 'inhuman' ways; hackers have the potential to defeat

notions of technological determinism by being able to master and direct technology for their own purposes (the 'hands-on imperative'). The lack of a mainstream level of recognition and influence, raises questions about the way in which society responds to sub-cultures that contribute towards the development of a technology.

Within the general social shaping approach, Latour's comparison of technological change with the political intrigues of Machiavelli's The Prince, provides a useful theoretical framework from which to examine the particular case of hacking. 'The Prince' is a name given to "describe at once machines, and machinations, techniques and society" (Latour 1986: 4). It is the anthropomorphisation of the various ways in which power is gained in society. Machiavelli's original Prince lived in a largely non-technical age where power was almost exclusively exercised by means of social ties. Men exerted power over other men in a hierarchical system of loyalties and obligations from which the social order sprang. Machiavelli's The Prince investigates the strategies and duplicity necessary to gain and consolidate this power in the face of numerous enemies threatening the stability of the social order. The issue of power is a perennial quality of human life, but in the modern technological world the means by which it is exercised includes, not just social ties, but the enlistment of 'non-human' allies as well, in the form of technological artefacts. The anthropomorphisation of the exertion of power, both social and technical, in the form of the Prince, is an attempt to describe the complex process whereby modern socio-technical systems exhibit deterministic tendencies: an identifiable trajectory of development.

In the social shaping tradition of 'getting inside the black box of technology', Latour argues that the apparent irreversibility of technology should not be accepted unopposed. The portrayal of 'The Prince' conceptualises a focus of power and control over technology that can be then be opposed by those seeking to prevent irreversibility. His injunction is to occupy the 'space' of the Prince. The artefacts that confront those wishing to do so are not the sine qua non of power. Their ability to reinforce the power of the Prince

is underscored by a series of social relationships without which they are obsolete. The Prince's medieval communal mill's importance as an instrument of social power rests upon the fact that he can coerce people into using it rather than their own hand mills: "The hardware is only the shadow of the technical plot" (Latour 1986: 17). The plot consists of various attempts by the Prince to create from the process of technological change, what Latour terms "inertia and automatism". Hackers are actors who consistently challenge these "two most common cliches about technology" (inertia and automatism). Hacking may be seen as an attempt to answer Latour's call to "occupy the space of the Prince".

(i) Inertia

Once a technology is closed to social shaping forces it readily assumes the quality of inertia, that is, it appears to be on an irreversible, autonomous trajectory of self-direction. Latour emphasises the fact that accretions of irreversibility, eventually leading to closure, are a result of the deliberate action of the dominant social groups aimed at preventing alternative interests redefining technology in line with their particular interests. Latour's crucial point is that regardless of how inertial technology appears to be to those human actors affected by it, at every stage of the technology's development, choices have been made that have shaped it. These choices are made by human actors whom Latour labels 'Sartrian Engineers'. These engineers he describes as 'Sartrian', "because they are free to choose even what will limit their freedom" (Latour 1986: 19). Technological trajectories are seen as a by-product of a Scrabble-like game between these engineers: just as a scrabble player is limited in his options by the words already placed on the board so engineers are sometimes faced with a technological fait accompli. "Irreversible technical constraints" can in fact be produced but these are not seen as evidence of technological determinism, rather, "It must be realized that part of the game is for each engineer to limit the freedom of movement of a later one...

Thus, in the end, a weaker engineer might find him or herself confronted by something that looks indeed like an irreversible fatum" (Latour 1986:18).

(ii) Automatism

Automatism is the notion, closely related to 'inertia', that technology's pervasiveness makes attempts to shape it to one's own aims futile. Its proliferation increases feelings of powerlessness and is achieved by a particular strategy of the Prince: the enlisting of non-human allies in an attempt to increase power and limit opposition. An example is the way in which the replacement of Police officers to direct traffic with traffic lights, enables authority to be exercised more subtly and pervasively than previously possible.

3.5.1 Hackers and the Prince

It is the accretion of individual choices by human actors in conjunction with the spread of automatism that eventually leads to people perceiving themselves to be dominated by technology's autonomous logic. Latour describes how this process can take on the aspect of a "socio-technical imbroglio" (Latour 1986:19) and how, "the mega-machine becomes bigger. Time, that is, irreversibility, is being constructed" (Latour 1986: 23). It is against such a project of closure that hackers will be shown to be fighting.

They are an example of a group that are unconvinced that computing should be received unquestioningly as a black box, and subsequent chapters trace the course of the closure process whereby attempts have been made to 'transform' computing: to convince people that the hackers' ability to get inside the black box should be prevented:

> The two most common cliches about technology, its inertia that would be too strong for anyone to resist, and its inner complexity that would be too much for anyone to fathom, are

> real enough, not as the **cause** of the Prince's moves, but as the **effects** that the Prince strives to achieve ... The first principle of technical democracy is thus never to offer this goal to the Prince on a golden plate (Latour 1986: 24).

Hacking is therefore an opportunity to analyse some of the Prince's moves in sharper relief than that which circumstances normally allow. The conflict between the establishment and computer users seems to be an ideal juncture at which to address questions of technological determinism and the alleged Machiavellian manipulations of the Prince. It is a fertile ground for enquiries into the process Latour describes as *translations*: the negotiations and various strategies, including acts of persuasion and violence, by which the establishment seeks to gain authority and power. Hackers provide an ideal location from which to embark on an enquiry into this realm: "science and technology are politics pursued by other means...the only other way to pursue democracy is to get inside science and techniques" (Latour 1986:25), an injunction that seems tailor-made for the hacker-ethos.

The subsequent chapters of this thesis form a detailed illustration of the translations that have occurred within computing and which the computer underground have sought to oppose. All the elements of Latourian technological change can be seen in the conflict between hackers and the dominant groups within computing. The way in which both sides of the hacking conflict translate the aims of their struggle into a language of persuasion using words and metaphors with emotive connotations, for example, is in keeping with Latour's emphasis upon the way in which "an actor bends space around itself, makes other elements dependent upon itself and translates their will into a **language** of its own" (Latour 1981: 286) (emphasis mine).

A crucial question for the Latourian view is the extent to which it is applicable to a political world where macro institutions and structures such as the state exert a sizeable constraining influence over individuals' attempts to shape technology to their own

purposes. Thus Williams and Russell point out that such an approach:

> leads, paradoxically, to a view of technological development as much more malleable than is the case. It overstates the power and autonomy of local actors, which are seen as capable of imposing their will. There is no explanation of the **external conditions** [emphasis mine] under which the attempt will fail ... Perversely this 'over-politicised' view of technology-an overblown significance accorded to scientists and technologists as shapers of society-(re)creates a form of technological determinism (Williams and Russell 1988:9).

The question for such groups as hackers, remains one of how to correctly place them in this interplay between negative macro-induced constraints and positive, potentially world-changing micro-originated actions. In one respect, they seem to be a development and response to the, "context of already strongly-articulated economic and social interests" (Williams and Russell 1988:10), prevalent within computer science. We see in the following sections, for example, the way in which they oppose the tendencies within society towards the privatisation of information and their subsequent claims to represent an alternative cultural view of computing. Hackers are thus receptive to an analysis which takes macro constraints into account whilst also illustrating their micro-level ability to change. Both parts of this approach are needed in order to avoid the pitfall of some micro-sociologists who indulge in, "opening up the black box and getting inside it, so to speak, only to close the lid behind them" (Williams and Russell 1988: 6).

3.6 THE CHANGING ECONOMIC NATURE OF INFORMATION

One of the more obvious effects of recent technological advances is the apparent threat such changes have made to traditional concepts such as the economic qualities of information.

Unlike other commodities, information has the usual economic costs of creation but practically zero reproduction costs. It also seems to be a 'commodity' which is particularly susceptible to increasing returns to scale within its production which lead to a tendency for large monopolies to exist within information processing.

The reason for both these qualities is the fact that: "the creation of any new knowledge, regardless of the creativity involved, requires a once and for all outlay of time and effort which does not need to be repeated, and is quite independent of the extent to which that knowledge is subsequently put to use. A greater demand spreads the fixed costs of creation over a greater information output" (Metcalfe, 1986:44). This creates increasing returns to application (substituting for the usual economic phrase, returns to scale), and thereby generates the natural tendency towards monopoly conditions within the information-creating activity. Such monopolistic tendencies go beyond just economic significance and create extra political significance when one considers the increasing returns to scale as they apply to government-sponsored communication networks and data bases. Large national communication networks tend to have an infrastructure administered as a nationalised industry or increasingly as a private firm granted conditional monopoly status. This creates the possibility of a communications system more conducive to central control and the surveillance of individuals[13].

A second peculiarity of information as a commodity, is the inherent uncertainty that exists in the links between efforts and outcomes and outcomes and market demand. Uncertainty in the demand for any commodity is inevitable due to the very nature of a market place. In economics, the market is said to imitate an auctioneer matching available demand with available supply, the coincidence of the two amounts giving the equilibrium price. The process whereby equilibrium is achieved, however, is impersonal

---

[13] Individual evidence of which is given later by Robert Schifreen - The Prestel Hacker.

and not conducive to advance planning, thus creating inevitable uncertainty as to the exact position of the eventual outcome.

With the case of information, however, the uncertainty arguably enters a new qualitative dimension. All knowledge is risky in an even more fundamental sense, namely that the eventual utility of information can only be fully ascertained *de post facto*: once the information has actually been put to use. In economic jargon, there is no stable production function, that is, the costs of producing information may be more or less than the value of the product once it actually reaches the market. In addition, the production of normal commodities, even if the ultimate price and eventual degree of utility are not known, at least has the benefit of the fact that the resulting product has some sort of value stemming from, if nothing else, the fact it is made of some sort of physical, material product. Immaterial information, however, has the danger that it will prove to be of absolutely no value to anyone.

This lack of certainty is a major reason why generally investments in knowledge creation such as science research are publicly funded. Risk is also apparent on the side of the buyer too, in so far as the nature of information clearly is not entirely known before it is purchased. These two peculiarities of information both point towards the inherent difficulty of establishing property rights in information and by extension computing, and linking rewards to effort, a cornerstone, (at least ideologically), of capitalism. In short, problems are experienced because, "uncertainty regarding outcomes and their valuations diminishes the incentive to engage in information creating activity, while the fact that knowledge is more costly to create than to communicate or imitate means that those who do not generate the knowledge may still capture a share of the rewards from application" (Metcalfe 1986: pp 44-45).

The basic, most important non-market peculiarity of information lies in its public good nature. Most economic commodities derive their prices from their scarcity. An element of this scarcity is the quality most commodities have which is that of rivalry in use, which simply refers to the fact that scarcity tends to

result from the fact that more than one person wishes to consume a single good. Information, however, is such that the term commodity does not seem to adequately apply. There is a fundamental lack of rivalry in use. If it is to be looked at as a commodity, then it is has the unique characteristic of its quantity not being reduced by consumption. The problem for the capitalist market therefore is that there is a need to obtain a revenue from the production of information by differentiating the market for it and excluding certain sectors of the market, allowing access to the information only if they are able to pay.

Within IT there have been two attempted solutions to this problem. One attempt has been to limit physical access to information where it is in a non-durable form. Examples of this would be the viewing of professional sports or the performing arts, and the scrambling of satellite and cable services. The general purpose in all these areas is to create a barrier to the informational good you are providing which a potential viewer can only overcome by paying for access to it. This technique recreates rivalry to access and generates a revenue base. The other attempted solution is where information is embodied in durable objects which are themselves private goods, for example, books, video recordings, and computer software in the form of floppy discs. The sale of these durable assets gives some sort of commodity status to information, provides a revenue base and is therefore a reward for creativity. However, as we have seen computer-generated information tends not to have as many opportunities for establishing such rivalry in use. Those wishing to do so are faced with the problem of imposing property rights on a commodity which has intrinsic potential to be used in a non-proprietary way. This leads to a situation whereby those attempting to impose property rights in information are confronted by those who recognise its non-proprietary potential.

The increasing tendency to privatise information is in keeping with wider privatising trends within market societies as a whole. Satellite and cable television are marketed with the emphasis placed upon the consumer watching their individually expressed preference

of entertainment free from any 'contamination' by such concepts as public broadcasting[14]. More vividly still, Umberto Eco[15] amongst others describes what he sees as the increased tendency of American buildings to minimise, within their original design, the concept of public space by following a fortress-like architectural style. New self-contained and fenced-off communities are springing up that have a similar appearance to medieval walled cities. Hackers, and their desire to freely access and share information represent an alternative interpretation of information with respect to the above market-orientated account.

3.7 CYBERSPACE - THE REAL AND VIRTUAL WORLDS

The most radical conceptualisation of the change in the nature of information is the notion of 'cyberspace'. It has fuelled hackers alternative interpretations of information's political and economic qualities. One of the immediate causes of conflict between hackers and the authorities is that the former view the systems of the latter as something of a 'playpen area':

> Cyberspace is *not real* ! ... Hacking takes place on a screen. Words aren't physical, numbers ... aren't physical ... Computers *simulate* reality, such as computer games that simulate tank battles or dogfights or spaceships. Simulations are just make-believe, and the stuff in computers is *not real.* Consider this: If 'hacking' is supposed to be so serious and real-life and dangerous, then how come nine-year-old kids have computers and modems? You wouldn't give a nine-year-old his own car, or his own rifle, or his chainsaw- those things are 'real' (Sterling 1993: 84).

This 'virtual reality' of computer data-bases has been fictionalised in the work of William Gibson, almost required reading

---

[14] Future mooted developments within cable T.V. promise interactive viewing qualities whereby the viewer can choose from a selection and combination of camera angles. This will have the effect of further personalising the viewers experience of an event.

[15] Eco Travels in Hyper-reality (1986)

for those interested in computer underground issues. In his science-fiction short story collection, Burning Chrome (1986), he gives the following description of both cyberspace also referred to as the matrix, and cyberpunks, the hackers of cyberspace:

> Bobby was a cowboy, and ice was the nature of his game, ice from ICE, Intrusion Countermeasures Electronics. The matrix is an abstract representation of the relationship between data systems. Legitimate programmers jack themselves into their employers' sector of the matrix and find themselves surrounded by bright geometrics representing the corporate data. Towers and fields of it ranged in the colorless nonspace of the simulation matrix, the electronic consensus-hallucination that facilitates the handling and exchange of massive quantities of data. Legitimate programmers never see the walls of ice they work behind, the walls of shadow that screen their operations from others, from industrial-espionage artists and hustlers like Bobby Quine. Bobby was a cowboy. Bobby was a cracksman, a burglar, casing mankind's extended electronic nervous system, rustling data and credit in the crowded matrix, monochrome nonspace where the only stars are dense concentrations of information ... (Gibson 1986: 197).

The information cyberspace represents is owned by huge multinational companies known as 'zaibatsus'[16]. The way in which hackers' activities are devoid of normal geographical and time constraints heightens their appreciation of, and affinity with, the cyberspace notions of information. The image of hackers as pioneers on a new frontier of immateriality is explicitly developed by John Perry Barlow:

> Cyberspace in its present condition has a lot in common with the 19th Century West. It is vast, unmapped, culturally and legally ambiguous, verbally tense (unless you happen to be a court stenographer), hard to get around in, and up for grabs.

---

16 'Zaibatsu' is a new addition to the latest edition of the New Shorter Oxford English Dictionary, it derives from the Japanese 'zai' meaning wealth and 'batsu' meaning 'clique'. (David Lister: The Independent pg 1, Tues 24 August, 1993)

> Large institutions already claim to own the place, but most of the actual natives are solitary and independent, sometimes to the point of sociopathy. It is of course, a perfect breeding ground for both outlaws and new ideas about liberty ... In this silent world, all conversation is typed. To enter it one forsakes both body and place and becomes a thing of words alone (Barlow 1990: 45).

These 'new ideas about liberty' refer to the ethical issues that 'cyberspace' raises for informational property rights. The case that new technologies go hand in hand with unconventional interpretations of their uses is put by the protagonist of Neuromancer: "burgeoning technologies require outlaw zones, that Night City wasn't there for its inhabitants but as a deliberately unsupervised playground for technology itself" (Gibson 1984: 19). Cyberpunk fiction portrays this 'unsupervised playground for technology' in the context of a dystopian future redolent with the fears of technological determinism: in both the sense of technology's inexorably autonomous trajectory and in fears of its dehumanising powers.

3.7.1 Cyberspace and technological domination

(i) Domination of the individual

Levy describes how the earliest hackers "attained a state of pure concentration ... When you had all that information glued to your cerebral being, it was almost as if your mind had merged into the environment of the computer" (Levy 1984: 37). Cyberspace represents this juncture of the qualitative evolution of information and the human interaction with the machines that process it. Hackers of the future are typically portrayed as the ultimate extension of this idea of man/machine symbiosis: "Certain central themes spring up repeatedly in cyberpunk. The theme of body invasion: prosthetic limbs ... genetic alteration. There is the even more powerful theme of mind invasion: brain-computer interfaces,

artificial intelligence, neurochemistry - techniques radically redefining the nature of humanity, the nature of the self" (Sterling 1986: xi).

Levy foresaw cyberpunk's depiction of the man/machine symbiosis with his observation that "Real optimum programming, of course, could only be accomplished when every obstacle between you and the pure computer was eliminated - an ideal that probably won't be fulfilled until hackers are somehow biologically merged with computers" (Levy 1984: 126). The earlier description of Chip Tango 'attaching his consciousness' to a process and 'butterflying his way across the net' also has connotations of such biological merging, and implies that hackers capable of similar merging are also capable of controlling computers at will. Later fieldwork evidence from hackers describes their experiences of accessing information as similar to 'drugs running through an addicts veins'. One US hacker, Eric Coggans, former member of the group known as the Legion of Doom, describes his relationship to the information contained on computers as that of 'a junkie in need of a fix' (Coggans: e-mail interview).

Cyberpunk's fictional depiction of cyberspace and what it is to mentally 'jack into' its matrix of information predicts, in language similar to the imagery of addiction used by hackers, an ultimate inability to control something that is inherently non-human:

> he closed his eyes ... It came on again, gradually, a flickering, non-linear flood of fact and sensory data, a kind of narrative conveyed in surreal jumpcuts and juxtapositions. It was vaguely like riding a rollercoaster that phased in and out of existence at random, impossibly rapid intervals, changing altitude, attack, and direction with each pulse of nothingness, except that the shifts had nothing to do with any physical orientation, but rather with lightning alternations in paradigm and symbol system. The data had never been intended for human input (Gibson 1986 a:40).

Thus cyberspace can be viewed as part of the tradition of writers who express the technological determinst fears that technology dehumanises people and its progress is uncontrollable.

(ii) Cyberspace and technology's autonomous trajectory

In addition to its portrayal of technology's dehumanising effects for the individual, Cyberpunk reinforces technologically deterministic views about the nature of the more general process of technological change. Sterling in his preface to Gibson's collection of short stories, Burning Chrome, argues that:

> In Gibson's work we find ourselves in the streets and alleys, in a realm of sweaty, white-knuckled survival, where high tech is a constant subliminal hum, 'like a deranged experiment in social Darwinism, designed by a bored researcher who kept one thumb permanently on the fast-forward button. Big Science in this world is not a source of quaint Mr Wizard marvels but an omnipresent, all-permeating, definitive force. It is a sheet of mutating radiation pouring through a crowd, a jam-packed Global Bus roaring wildly up an exponential slope. These stories paint an instantly recognizable portrait of the modern predicament (Gibson 1986:11).

The protagonists of Gibson's fiction give the sense that even though they may be technically literate in the workings of the environments they find themselves in, their experiences result in them having increasingly less control over their eventual fates.

3.7.2 Cyborgs: a rejection of Technological Determinism

Cyberpunk explores the implications computing technology has had for conceptualisations of information's changing qualities. It gives a fictional account of a group dealing with the blurred boundary between the material and immaterial nature of information and has empirical significance in so far as it has

relevance to hacking as a real world phenomenon. Cyberpunk's treatment of the changing boundaries of information is extended to the blurring of the boundaries between the organic and inanimate by Haraway's concept of the 'cyborg': "A cyborg is a cybernetic organism, a hybrid of machine and organism, a creature of social reality as well as a creature of fiction ... but the boundary between science-fiction and social reality is an optical illusion ...". (Haraway 1985:174). Because of cyborgs:

> certainty of what counts as nature - a source of insight and a promise of innocence - is undermined, probably fatally ... Who cyborgs will be is a radical question, the answers are a matter of survival. Both chimpanzees and artifacts have politics, so why shouldn't we? ... taking responsibility for the social relations of science and technology means refusing an anti-science metaphysics, a demonology of technology ... (Haraway 1985:177).

Haraway endorses theoretical attempts to analyse the political implications of artefacts in the process of technological change. Whilst Latour refers to the conflict between the Prince and his adversaries, Haraway describes how, "the relation between organism and machine has been a border war ... This essay is an argument for pleasure in the confusion of boundaries and for responsibility in their construction" (Haraway 1985:174). Hackers are a prime example of a group enjoying the pleasure Haraway prescribes. The next section examines how this then characterises them as a group opposed to the status quo.

3.7.3 Cyberspace and the culture of opposition

The sense of powerlessness that accompanies cyberpunk narratives raises doubts as to the potential of cyberpunks (and by implication their real world representatives, hackers) to be a meaningful focus for cultural opposition to the establishment's control of technology. Cyberpunk has been dismissed for "its

resexing of the 'neutered' hacker in the form of the high-tech hipster rebel" (Ross 1990: 145). Cyberpunk is accused of being rooted in the fears of the white male middle-classes rather than being based on a realistic cultural force. It is criticised as feeding off:

> the phantasmatic street diet of Hobbesian lawlessness and the aesthetic of detritus that is assumed to pervade the hollowed-out core of the great metropolitan centers. This urban fantasy, however countercultural its claims and potential effects, shared the dominant, white middle-class conception of inner-city life. In this respect, the suburban romance of punk, and subsequently, cyberpunk, fashioned a culture of alienation out of their parents' worst fears about life on the mean streets (Ross 1991:146).

Some writers, however, do find within cyberpunk a vestigial description of hacking culture's potential as an oppositional force. Cyberpunk can be viewed as a portrayal of the amalgamation of the technological knowledge of hackers with the anti-establishment ethos of the punk-rocker. The potential for this amalgamation to produce a source of opposition to the dominant social constituency is aided by the fact that technology is now more readily accessible and manipulable than in previous times when it was more easily subjected to institutionalised control:

> times have changed since the comfortable era ... when Science was safely enshrined - and confined- in an ivory tower. The careless technophilia of those days belongs to a vanished, sluggish era, when authority still had a comfortable margin of control. For the cyberpunks, by stark contrast, technology is visceral. It is not the bottled genie of remote Big Science boffins; it is pervasive, utterly intimate. Not outside us, but next to us. Under our skin; often inside our minds. Technology itself has changed. Not for us the giant steam-snorting wonders of the past ... Eighties tech sticks to the skin, responds to the touch ... (Sterling 1986: xi).

3.8 HACKING AS AN ALTERNATIVE CULTURE

Hackers more than any other group of people epitomize what it is to interact with a machine. It remains an open question, however, whether hackers' technical competence is one of humankind's last forms of defence against an ever more baroque, complex yet centralised technological world: or whether they have lost control of themselves as a reaction to the seduction of technology's 'powers'. To put the issue more bluntly, computer subcultures are perhaps one of the last of what Marcuse terms 'alternative cultures'. They offer the promise of opposition to technological determinism and the machinations of the Prince:

> the CU reflects an attempt to recast, re-appropriate, and reconstruct the power-knowledge relationship that increasingly dominates the ideology and actions of modern society ... we interpret the CU culture as a challenge to and parody of conventional culture, as a playful attempt to reject the seriousness of technocracy, and as an ironic substitution of rational technological control of the present for an anarchic and playful future (Meyer and Thomas 1989 a:1-2).

In keeping with this portrayal of hackers encapsulating forces of opposition, increasingly "the elitist class profile of the hacker prodigy as that of an undersocialized college nerd has become democratized and customized in recent years; it is no longer exclusively associated with institutionally acquired college expertise, and increasingly it dresses streetwise" (Ross,1990:26). However, the fact that the CU is an underground movement may inherently limit the political impact hackers have:

> They find it hard to make any remotely convincing case for their actions in front of the general public ... But if they speak out too loudly and publicly, they will break the fragile surface tension of the underground, and they will be harassed and arrested. Over the longer term, most hackers stumble, get

> busted, get betrayed, or simply give up. As a political force, the digital underground is hamstrung (Sterling 1993: 230).

Sterling's characterisation of hackers as a group whose oppositional status makes them intrinsically reluctant to 'break the surface tension' of the underground is recognised within the CU. Hackers' necessarily underground status does not inevitably lead to them being 'politically hamstrung', it can also seen as their political advantage:

> The worst thing the underground could do now is organise on a mass level. Our strength is to be found in that we are a mass of atomic entities operating against a concerted attack. The attacks on the Underground by the witch-hunters may smash a few individuals here and there, but the overall body lives on. Just as the United States Army failed to fight effectively against a dispersed phantom force like the Vietnamese, so too will the onslaught fail against a patternless weaving of hackers. What the opposition is trying to do is like trying to shoot gnats with a shotgun. As long as the Underground remains dispersed and loosely organized, there is no way they can search out and destroy the entire bunch of us. If we band together, then of course, they have much larger target (The Dark Adept 1990).

Molina (1989) describes 'dominant social constituencies' as being the prime agents that dictate the pace of that change. Hackers and their 'geeky' image might be perceived as an unusual choice of a group with pretensions to contest this domination. A further complicating aspect of hacking is the degree to which hackers oppose dominant social forces within computing whilst at the same time containing their very traits. Thus, whilst generally opposing trends towards the increasing commodification of information and by extension the ethics of the free market, some hackers at least, almost personify market values, leading to the claim that they are not an alternative culture at all:

> the hacker cyberculture is not a dropout culture; its disaffiliation from a domestic parent culture is often manifest in activities that answer, directly or indirectly, to the legitimate needs of industrial R and D. For example, this hacker culture celebrates high productivity, maverick forms of creative work energy, and an obssessive identification with on-line endurance (and endorphin highs) -- all qualities that are valorised by the entrepreneurial codes of silicon futurism ... The values of the white male outlaw are often those of the creative maverick universally prized by entrepreneurial or libertarian individualism ... teenage hackers resemble an alienated shopping culture deprived of purchasing opportunities more than a terrorist network (Ross 1990: 90).

The political status of hackers as an oppositional subculture is thus debateable. The comments made by Hayes illustrate some of the concerns writers have about the potential ambivalence of the hackers' position: their actions are rooted in opposition to the dominant social constituency in control of computing, yet they exhibit other tendencies which leave them open for absorption into that dominant social constituency. This is perhaps an inevitable result of the fact that hackers utilise the very technological artefacts that the dominant social constituency relies upon to facilitate its control over power. What is less ambiguous about hackers is the way in which they turn on its head, the usually negative counter-cultural response to technological progress, instead of demonising artefacts, they prefer to use them to their fullest advantage. Hackers' more specific claims to be an alternative culture rest with their instinctive dislike for government information-gathering bureaucracies, which they perceive to be encouraging the privatisation of information.

3.8.1 Opposition to commodification

> *Control of information by government is no longer possible. Indeed, information is now transnational. Like money, it has no fatherland* (Denning D. 1990).

It's as if big companies and their suck-up lawyers think that computing belongs to them, and they can retail it with price stickers, as if it were boxes of laundry soap! But pricing 'information' is like trying to price air or price dreams (Sterling 1992: 85).

The complexity and difficulties encountered by the market economy in attempting to impose intellectual property rights are reflected in its struggle with hackers. Information and its specific, and in some respects unusual, economic properties can be seen as part of a wider social phenomenon whereby conflicting groups struggle and negotiate over whose view of information will ultimately prevail. The opposition to market pressures to commodify information and enforce property rights can be seen in two distinct realms: software production and computer systems intrusion. The more obvious form of hackers' oppositional status is their failure to respect the copy-protection methods used to assert it. The Software Publishing Association estimates that software producers lost approximately $1 billion in sales in 1986 as a result of unauthorised copying (both for profit and for personal use)[17].

Companies that have attempted to challenge the corporate emphasis placed upon information's marketability have ended up operating within the ground rules of the capitalist approach to software. The Apple Computer Company, for example, was so named because it was conceived as a wholesome, politically liberating, user-orientated, alternative to corporate computing. Despite its original aim, it too became part of the corporate culture it was established to oppose. However, there remains a groundswell of opposition to the corporate commodification of information from such people as Richard Stallman and his GNU project. GNU stands for Gnu's Not Unix[18]. In essence the GNU system is a completely Unix-compatible system, the major difference being that as Stallman says about his

---

[17] c.f. Peláez,1990:6

[18] A general-purpose operating system particularly popular in academic environments

creation, "I am writing so that I can give it away free to everyone who can use it" (Stallman, 1985: 1). The GNU manifesto is important because it contains crucial elements of what Levy identifies as the earliest hacking ethic and its accompanying antipathy towards the commodification of software.

The GNU Manifesto

1) RATIONALE.
"Software sellers want to divide the users and conquer them, making each user agree not to share with others. I refuse to break solidarity with other users in this way. I cannot in good conscience sign a nondisclosure agreement or a software license agreement" (Stallman, 1985: 2)
2) BENEFITS TO USERS.
"Once GNU is written, everyone will be able to obtain good system software free just like air". [*ibid*: 3]
The specific advantages of this are that,
a) "Much wasteful duplication of system programming effort will be avoided. This effort can go instead into advancing the state of the art." (*ibid* : 3)
b) Source codes are freely available, which will mean that users will be free to make program application changes to suit their individual needs without interference from copy-right litigation worries.
c) Free availability of source code tends to lead to a better educational environment for further software development.
d) The legal costs of implementing copy-right protection are eliminated.
3) BELIEFS.
"Copying all or parts of a program is as natural to a programmer as breathing, and as productive. It ought to be as free." (*ibid* : 4)

3.8.2 Hacking as anti-bureaucratic rebellion

An aspect of the modern technological order is the individual's

perception of anonymity in the face of large commercial entities. Acts which manage to express individuality become valued as human blows struck against dehumanised and unaccountable bureaucratic structures. Hacking as a form of rebellion can take both macro and micro forms. On a macro-level, Steve Hardin argues, "most law-abiding people fantasize about breaking the law big-time and getting away with it. We "ordinary folk" are intrigued by the little guy who beats the big corporations or governments" (Hardin: e-mail interview). The anti-authoritarian outlook of hackers which is needed as part of their 'free information' ethos tends to encourage little empathy with governmental agencies. The president of the French Chaos Computer Club, Jean-Bernard Condat, who partially began his career as an act of political rebelliousness, relates how:

> When I was 16 1/2 years old, I finished the "lycee" and passed without any problem my "bacculauret." I go from Beziers to Lyon (middle of France) for my University ... and discover that all the information will easily be available on a host in Palo Alto (California, USA). I try to connect me from my University-room and work on my poor $53.00-TTY-terminal all the nights. One night, I have the visit of the great DST service (anti-spy service) that ask me kindly "Explain us how you do for connecting you..." I never answer correctly to this question, and enter the same day in the CU (Condat: e-mail interview).

The dislike many people have for large 'faceless' bureaucratic organisations adopts a specific manifestation with hackers whose failure to have ethical qualms about obtaining free communication services is encouraged by what they perceive to be the unjustified level of the firms' monopoly profits: (Sterling 1992: 62). Activities which involve the avoidance of payment for communication services are further encouraged by a belief that no 'real' cost is being incurred by the victim company. Ralph and Maelstrom a Dutch and US hacker respectively, both emphasised that any pecuniary losses attributable to their activities were carried not by individuals but by an unscrupulous monopoly power. Maelstrom, for example, in

describing the activities of the German hacking groups Red Sector Inc.[19] mentions the use of stolen AT&T card numbers but qualifies the use of the word 'stolen' by contending that:

> You can't 'steal' a number without stealing the whole card; you can only copy it. The rationale was that the customer whose card is being abused won't have to pay the bill, AT&T will absorb it and give him/her a new one. And AT&T deserves to absorb. After all what does it cost to make a phone call? The lines are already in place, and the electrons don't care how far they travel. The voltage is going through your lines whether you use it or not. So you're not really ripping anyone off. Big companies like AT&T just like to make it seem that way so they can get more money (Maelstrom: e-mail interview).

On a more micro-level Rop Gongrijp points out how hacking can be in response to the bureaucratic inconveniences imposed on computer users:

> I gave you the example of the VMS system where the operating system itself has all these little windows and forms built in ... many for the sake of the internal bureaucracy and if you program around that, you can hack the system, because one of the many purposes of those windows is to keep you out, but the other advantage of programming around that, and that's been done quite a lot by very respectable programmers, and the techniques are used in most professional pieces of software, especially for IBM machines. If you hack around that window, that whole bureaucratic system, your file access becomes faster, you can do more things with the system, you can write software that genuinely looks more impressive, because it's much faster than anything that's written in the official way, and in DOS that's very, very well known (Gongrijp: Delft interview).

'Mercury' also emphasised the positive aspects of hacking which can be used to defeat bureaucratic inertia and the obstructions

---

[19] c.f. Chapter 7 for full details

thrown up by the exigencies of day to day commercial life. He argued that he benefited from hacking because it helped him in his:

> learning how operating systems work and how to scrounge for resources. I work for a multinational corporation. In fact, there is a gulf between the home office and those of us 'foreigners' in the field. This means that we do not always receive engineering change orders or detailed schematics or software manuals. Having learned about computing from trying things on a wide variety of systems and having acquired a 'sense of the system' I have been able to hack our own computers. The need here is varied. My job is to train users of our systems. Ideally, I guess, I would merely parrot the words of my bosses. In fact, the users feel a need to know more about what is under the surface. Therefore, I have been able to help the clients of my employers by knowing how to get beneath or around security (Mercury: e-mail interview).

The exploits of people such as Captain Crunch[20] give rise to the tacit respect and recognition that the technologically unversed majority hold for acts involving illegal but technically dexterous methods. Edward Pfuhl[21] refers to this phenomenon as the "Rust effect", named after the young West German solo pilot who breached Soviet Air defence systems. Respect tends to be afforded for any non-violent feat that involves a technological artefact being used to defeat a technological system, especially if that system, is part of '*the* system'. Human individuality is perceived as threatened by the anonymity of modern technological systems, those that are seen as striking back against that anonymity are more difficult to view as criminals than would those acting against identifiable individuals using less technological means.

---

[20] John Draper alias "Captain Crunch" achieved notoriety because he serendipitously found that by whistling into a phone with a toy whistle he could access on a global basis, telephone systems. The name derived from an American brand of breakfast cereal within which was enclosed the plastic child's whistle as a free gift. This discovery was due to the fortunate coincidence that the tonal quality of the whistle exactly matched the electronically coded whistles of the international telephone system which were used to limit access to its communication network.

[21] New York Times 20-21 April 1991

Hacking can be seen as "the necessary evil that will always be there; humans, by nature, will attempt to break the rules placed over them. And the anonymity of much of the computer underground activities make it that much more attractive" (Kehoe: e-mail interview). If hacking is sometimes fuelled by anti-authoritarian or anti-bureaucratic sentiments then ironically government attempts to reduce it may themselves be the raison d'être of further hacking. Richard Stallman identifies this anti-authoritarian stance, when asked whether he thought that some hacking was undertaken in a spirit of political rebelliousness he replied: "I don't see a connection directly with abuse of power by governments, but abuse of power on a smaller scale by sysadmins seems directly relevant". His emphasis was upon the behaviour of grass-roots system managers and administrators and contended that it is not enough just to prosecute and/or fix holes that hackers draw attention to, "neither of these would eliminate the motive for cracking. The way to do that is to stop the fascist behaviour which inspires blind resistance--to stop treating disobedience as if it were evil" (Stallman: e-mail interview).

3.8.3 Anti-Government Sentiment - privacy and double standards

A particular aspect of hacking's general anti-bureaucratic sentiment is its perception that it may represent one of the last safeguards against government intrusions of privacy made increasingly easy by the information-gathering capabilities of computers. Whilst the CSI emphasise that even hacking's element of 'harmless browsing' is unethical because of its accompanying invasion of peoples' privacy, hackers prefer to emphasise the almost total lack of privacy that exists in the modern electronic world and of which most people are ignorant:

> The concept of privacy is something that is very important to a hacker. This is so because hackers know how fragile privacy is in today's world ... In 1984 hackers were instrumental in showing the world how TRW kept credit files on millions of Americans. Most people had not even heard of a credit file

> until this happened ... More recently, hackers found that MCI's Friends and Family program allowed anybody to call an 800 number and find out the numbers of everyone in a customer's 'calling circle'. As a bonus, you could also find out how these numbers were related to the customer ... In both the TRW and MCI cases, hackers were ironically accused of being the ones to invade privacy. What they really did was help to educate the American consumer (Goldstein 1993: CuD 5.43).

They contend that the most pressing moral requirement is not to criticise those who highlight peoples' lack of privacy, but rather to improve security so that privacy can be re-established. In this context, disregard for property rights and privacy is viewed as a justifiable aspect of their drawing attention to the establishment's tolerance of lax security standards:

> I am not sold on the bourgeois liberal idea of 'privacy'. If you don't want your neighbors to know you can't cum unless your wife canes your bum, well don't do it in public. If you use a credit card to pay for a meal, you can hardly complain if your name shows up on a mailing list. Private is what you can keep in your head, your heart, your home. Three can keep a secret if two of them are dead. We live in an electronic fishbowl ... and yet, I'm still attracted to the words of Frank Lloyd Wright who designed houses for privacy, calling privacy 'the hallmark of civilization' noting that savages have no privacy (Mercury: e-mail interview).

Such a conflicting mixture of attitudes is mirrored in the concerns of other hackers. For example, Gongrijp and other members of Hack-Tic voiced their concern that encryption methods are not used frequently enough to ensure the privacy of e-mail communications, and that the available encryption keys have been compromised by the NSA's requirement that they be breakable[22].

---

[22] c.f for example, the NSA encryption debate covered in John Perry Barlow's: Decrypting the Puzzle Palace - Communications of the ACM June '92.

Such concern over privacy rights were also voiced by Martin Freiss a hacker from Paderborn in Germany:

> information freedom' is the slogan of most hackers over here (including the notorious CCC, chaos computer club). We already have a situation where electronic communications are unsafe, i.e. governments may legally tap data lines and make copies of electronic mail. Plus, the suspicion of 'hacking' alone (i.e. no evidence) is sufficient to get search warrants or to impound equipment. What hackers (not the kind that wilfully destroys data for the fun of it, but the real hackers) are fighting for, is something of a battle of principles. They want to keep the new electronic media as safe or even safer than regular paper mail from intrusion by government agencies (Freiss: e-mail interview).

Hackers argue that threats to privacy posed by government agencies are ignored, whilst at the same time, they are stigmatised because of the threats they are deemed to pose. This apparent double-standard fuels their belief that they are being victimised in a form of an alleged witch-hunt process. Concern over the possible actions of government agencies is not limited to hackers, however. The subject was raised during the parliamentary debate over the passage of the Computer Misuse Act: "The security services represent much more hacking than a few private individuals, yet they are not recognised in the slightest in the Bill" (Cohen, Hansard 1170: 9th Feb 1990). Added to the possibility of uncontrolled intrusions by government agencies is evidence of breaches of privacy made possible through the neglect of those responsible for ensuring privacy. Eric Howe the Data Protection Registrar, for example, has called for the removal of legal loopholes that allow banks and other organisations to be safe from prosecution when they have been deceived into giving out personal information by fraudsters pretending to be personnel authorised to receive the information[23].

---

[23] The Independent pg 4 15 July 1993.

Although the CSI has been vocal in its condemnation of hackers who interfere with other peoples' privacy privacy rights, there are several instances of the authorities using the same techniques that they have criticised in others. For example, System managers argue against hacking activity on the grounds that it is an invasion of the privacy of other users, whilst they retain the right to read other peoples' electronic mail, or tap their phones. That such instances occur may be partly due to the ease with which ethically dubious situations arise within computing. Robert Schifreen, the 'Prestel hacker' describes the extent to which his activities were monitored:

> It's pretty certain that my phone was being tapped. Once or twice I picked up the phone when it was tinkling and there were people talking on the other end saying things like "shall I record this John?" ... I heard it tinkling on a Sunday afternoon and it said "oh, sod it, I've got the wires in the wrong order". I also had an account on Telecom Gold, one of the commercial services run by BT, and there is a little known command on Gold known as stats or fstat, that tells you what files you've got open and I typed that once and it told me that I had a file open such that everything I typed was being copied to a mail-box called "security", and basically the security manager was logging my entire sessions and I phoned him up and he said "yes, well as part of my contract with you, BT is entitled to monitor selective lines, to guarantee quality of service" which the interception of communication act, specifically allows, and it then turned out that Steve Gold, my partner in crime was also having his box monitored so make of that what you will (Schifreen: London interview).

Morally ambiguous activities are thus on occasion sanctioned in certain instances, yet hacking is argued to be unequivocally wrong. Gongrijp points out that: "no boss can open up your private mail, no university can steam open your mail if it has your name on it, not without being in serious legal trouble if you find out, and yet every employer thinks he has the right to look at e-mail" (Amsterdam interview). Although recourse is made to arguments based on the premise that computer-stored data, and remotely accessed computer

systems should be treated as if they are physical property, system operators are accused of dropping such criteria in their own computing activity. Thus, Cosell a commercial systems manager who was one of the most vociferous of the CSI opponents to hackers encountered during the study, compared hacking to the joy-riding of cars: "Assuming you come out to the parking lot and your car is JUST where it was left, except maybe the engine feels a bit warm. How is this different than discovering that someone had logged into your computer?" (Cosell: e-mail interview). Despite the force of his moral view he also admitted that he:

> had to do this sort of thing once or twice over the years. I recall one incident where I was working over the weekend and the master source hierarchy was left read-protected, and I REALLY needed to look at it to finish what I was doing, and this on a system where I was NOT a privileged user [although I was an authorized ordinary user], so I 'broke into' the system enough to give myself enough privileges to be able to override the file protections and get done what I needed [at which point I put it all back, and told the sysadmin about the security hole] (Cosell: e-mail interview).

This experience is particularly interesting because of the way in which Cosell proceeds to imply (by his use of inverted commas) a break down of the applicability of a physical analogy when it is applied to his own action. The ease with which ethical quandaries can arise with the question of information is further illustrated by Bruce Sterling's account of his time spent 'trashing' whilst having been temporarily excluded from a particular session of a Federal Computer Investigations Committee (FCIC) security conference he was attending. Sterling proceeds his description of his act of trashing by commenting: "The legality of trashing is somewhat dubious, but it is not in fact flagrantly illegal". Backed by this 'lack of illegality' he proceeded to empty one of the trash baskets in one of the office-rooms opposite the security conference. Apart from finding a telephone-card bill from which he found out a woman's home

telephone number and a list of acquaintances' numbers that she had phoned, he also sellotaped together fragments of various drafts of a love letter she had written. At this stage in the account Sterling is aware that he was "Driven by motives that were completely unethical and prurient", yet this did not stop him from examining in detail the handwritten notes (Sterling 1993:198).

Despite the professed concerns hackers have with the issue of privacy, members of the CSI interviewed gave little credence to the idea that hackers represent legitimate or sincere concerns about privacy. The distance between the two groups on this issue is shown with such comments as: "System crackers take the 'public good' stand to try and justify their actions. I'd wager NOT ONE of them ever said, 'Hey, let's break into xxxx system tonight because I think they're violating the privacy rights of the local townfolk". Pardon the expression, but that's a lot of bullsh*t. It's a coverup - and a weak one" (Bob Johnson: e-mail interview).

3.9 CONCLUSION

This chapter has illustrated two main issues of control stemming from the concept of technological determinism. Firstly, there is the common complaint that 'technology is out of control'. This loss of control is seen as being exogenous to social factors, and it is experienced as an autonomous quality of the technology itself. The impact of its autonomous nature is viewed as one of domination, at both a micro and macro level, of the individuals and society that feel its impact. Secondly, there is the situation where loss of control over technology is the result of one set of interests within society exerting its power over another. This is the deliberate reduction of control where its loss is endogenously determined by societal factors deliberately limiting the control certain groups have over a technology. One group gains power through the control it has over technology, it thereafter attempts to practice 'closure', that is, it seeks to shape the technology so that groups undesirable to the original group are excluded from having any influence.

Hackers have been shown to have relevance in both of the above categories. In the first case, they have an intimate knowledge of, and close affinity with, computers. Technological theorists are often dispirited with the repeated tendency of technology to seemingly assume anti-human stances. They frequently call for an alternative cultural repository of new technological values that express mastery over, not subjugation to, artefacts. Hackers' ability to control technology for their own purposes is seen as evidence of human empowerment over technology's dehumanising tendencies. At the social level, therefore, hackers represent resistance to passive acceptance of technology and its impact. At the level of technology as it effects individuals, the close affinity hackers like Chip Tango have with computers has ambivalent implications for notions of technological determinism. This affinity can be interpreted as both evidence of individual control over technology, or alternatively, narcissistic dependence upon it. This issue is treated more fully in the next chapter, with its analysis of the role addictive behaviour plays in hacking.

Hackers disregard for informational property rights, combined with their technical expertise, offers hope for those seeking examples of technology being put to uses that run against the interests of dominant social constituency. The particular significance of hackers as a group involved in the process of technological change is that they offer a manifestation of 'technological politics' in action. The battleground of closure where hackers' claims to viability as an alternative culture reside, is the point where the competing interpretations of information meet. Hackers reject both the technologically deterministic implications that computing is beyond peoples' ability to control for their own ends, and also the notion that the control of it should be the sole preserve of dominant social groups wishing to assimilate it into the market economic order. They contend that the nature of information is fundamentally unsuited to attempts of commodification: it is 'like pricing air'. The chapter has identified the main problems encountered in attempting to enforce property rights over information. Hackers contribute to an

environment where free access to non-proprietary information is seen as both technically possible and ethically desirable by the CU. This forms the basis for group differentiation between themselves and the CSI. Whilst the CU professes its stance of free information for all, the CSI doubts its sincerity, preferring to judge the stance an ex post rationalisation of their 'alienated shopping culture', rather than an a priori motivating factor.

Whilst it would be naive to force the links between the work of William Gibson and the world of contemporary hackers, his notion of cyberspace and its cyberpunk denizens arguably does have some resonance with the computing environment as experienced by hackers. Within the information revolution, the notion of cyberspace provides an illustration of the process by which the nature of information is changing, and the implications of the process for both groups and the individual. The pertinence of Gibson's work rests upon the way his imagery can be seen as being metaphorically representative of both how individuals relate to the mass of data being produced by computers, and also the role of large contemporary communication organisations. The lack of respect and even feelings of antipathy held towards such companies as "Ma Bell" in the USA are held not just by those directly involved in the inventive manipulation of technological artefacts such as telephones and telephone systems. 'Ordinary people' with few technological skills seem to express resentment at the bureaucratic and monopolistic nature of IT firms. Zaibatsus may be an extreme characterisation, if not caricature, of modern communication companies, but the concept arguably provides an accurate, if not dramatic, representation of the contemporary public's perception of large institutional facelessness.

The greatest significance of notions such as cyberspace and cyborgs, is the way they highlight hacking's potential as a site for alternative cultural values. Evidence for the notion that hacking represents a repository of counter-cultural values is ambivalent. It is potentially accurate to the extent that it portrays the visceral approach hackers adopt to technology. This approach offers a

possible method for 'reducing the margin of control authority has over technology'. It promises to provide the basis of a political approach with which humans can confront the inertia induced by determinist perceptions of technological dominance. Cyberpunk, however, has also been dismissed as a projection of 'techno-masculinity' aimed at making up for the inadequacies of the 'neutered hacker'. An interpretation that throws doubt upon the concept that hackers, in either their real or fictional form, represent a meaningful challenge to establishment control. A fuller investigation of hacking culture is the subject of the next chapter which will help to ascertain the validity of hackers' claims that they embody alternative cultural values.

Chapter 4 - The hacking community: culture and motivation

4.1 INTRODUCTION
4.1.1 The hack
4.1.2 The hacker ethic

4.2 HACKING CULTURE
4.2.1 Hacking culture - specific elements
4.2.2 Hacking culture - male predominance
4.2.3 Reasons for paucity of female computer scientists

4.3 ACADEMIC MOTIVATION THEORIES

4.4 HACKERS' MOTIVATION THEORIES
4.4.1 Feelings of addiction
4.4.2 Curiosity- humans and technology
4.4.3 Boredom
4.4.4 Enjoyment of feelings of power -information for information's sake
4.4.5 Peer recognition

4.5 CONCLUSION

4.1 INTRODUCTION

After locating hacking within theories of technological change, this chapter begins the study's specific examination of the activity's status as an alternative cultural phenomenon. It explores those aspects of hacking that form the basis of its boundary-forming conflict with the CSI.

The empirical data in this chapter draws from my fieldwork of both e-mail and face-to-face interviews with hackers. The resultant findings make it apparent that hackers' reasons for hacking are more complex than the literature on the subject indicated. The main motivational aspects of hacking are described from an academic standpoint and thereafter largely from an internalist, hackers point of view. This is in preparation for the subsequent investigation of how hacking is perceived and construed by those external to it.

The motivations lying behind hacking, as described by the hackers themselves, are categorised into six areas. The first category, curiosity, is an essential prerequisite for the activity to begin in the first place, but it risks becoming the addictive behaviour described in the second category. The example used is that of Paul Bedworth, who was acquitted whilst charged under the Computer Misuse Act, on the defence that he was addicted to computers. The other categories form part of the complex interrelation of factors that influence hackers, different factors playing a variable role in the motivation of any one hacker. It is thus difficult to categorically gauge how representative of the hacking community such interviewees were, but those chosen tended to be relatively high-profile figures (based upon the number and apparently uncontradicted knowledgeability of their contributions to electronic magazines, and their reputation within the computing community). The quotations used are individual examples of opinions commonly encountered amongst a wide range of different hackers. Suitable emphasis is placed upon any of those quotations that appeared to be atypical in any way.

Groups within computing recognise that 'hacking' has changed its meaning from it's original usage[1]. Levy (1984) describes three generations of hackers who exhibited, to various degrees, qualities associated with the hacking's original connotation of playful ingenuity, epitomised by the first generation of pioneering computer aficionadoes at MIT's laboratories in the 1950's and 1960's. The phrase is now almost exclusively used to refer to unauthorised computer intrusions carried out by an addition to Levy's generations of hackers: the fourth generation. The study concentrates upon this generation, who are now vilified by the establishment, but who claim to represent a continuation of hacking's original values. The first generation of hackers were active in the development of the earliest software, the fourth generation have been criminalised by the passage of anti-hacking legislation. This evolution in hacking's role is explained in the study by its description of the closure process whereby the reduction of hackers' influence within computing is seen as the result of a social process of negotiation and conflict. This chapter's purpose is to present an internalist account of hacking which can then be compared later in the work with the externalist account. The ensuing conflict between the two interpretations is what fuels the process of closure.

Levy, and some of the hackers interviewed in this study, made the point that the phrase 'hacking' implies a potential quality of **any** technology. However, the word has now been used by the media to such an extent that its de facto definition more narrowly refers to anyone who attempts unauthorised access to a computer system. This reduction in meaning has meant that computers are at the fore-front of the media's perception of hacking. It has also resulted in a general lack of awareness that the breaching of computer systems seems to be but one aspect of a range of activities centred upon curiosity as to the workings of technological artefacts of varying degrees of sophistication. Such activities may also range from lock-

---

[1] c.f. Levy in Hackers: Heroes of the Computer Revolution (1984)

picking to phone-phreaking[2]. Whilst hacking may indeed contain such heterogenous roots, this study has been forced to adopt a more specific focus than would have been possible with such a broad-based definition. It has concentrated more narrowly on hacking in computing.

4.1.1 The hack

The basis of hacking culture is 'the hack'. The hack did, and still does in some quarters, refer to the performing of a neat programming trick. It is more widely defined as an attempt to make use of a technology in an original, unorthodox and inventive way, although it will predominantly refer to illicit break-ins and use of computer systems. Turkle (1984), categorises the main elements of the wider definition of illicit hacking, and the general mentality of those who hack in the sense of seeking to manipulate any technology for unorthodox means.

She refers to the "hack" as being: "the holy grail. It is a concept which exists independently of the computer and can best be presented through an example using another technology complex enough to support its own version of hacking and hackers" (Turkle 1984: 232). The example she uses is that of phone-phreaking and its main adherent is John Draper, alias Captain Crunch. The hack, in this instance, refers to such technological stunts as having two phones on a table; talking into one and hearing your voice in the other after a time-delay in which the original call has been routed around the world first.

Turkle interpreted this type of hack in the following manner,

> Appreciating what made the call around the world a great hack is an exercise in hacker aesthetics. It has the quality of [a] magician's gesture: a truly surprising result produced with ridiculously simple means. Equally important: Crunch had not

[2] Hackers at the headquarters of the Dutch group, Hack-Tic, also referred to gene-biology hackers and chemical hackers who they define as people who push their respective disciplines to the furthest limits.

> simply stumbled on a curiosity. The trick worked because Crunch had acquired an impressive amount of expertise about the telephone system. That is what made the trick a great hack, otherwise it would have been a very minor one. Mastery is of the essence everywhere within hacker culture. Third, the expertise was acquired unofficially and at the expense of a big system. The hacker is a person outside the system who is never excluded by its rules (Turkle 1984: 232).

The main characteristics of a hack are therefore identified as:

1. **Simplicity**: the act has to be simple but impressive.
2. **Mastery**: the act involves sophisticated technical knowledge.
3. **Illicitness**: the act is "against the rules".

The hack and the heterogenous 'kick'

In addition to the elements identified by Turkle is the characteristic eclectic pragmatism with which hackers approach **any** technology. Apart from Levy's very early recognition in Hackers that hacking involved such diverse activities as lock-picking and model-railway maintenance (and the accompanying tinkering with gadgetry that this involves) hackers themselves express the wide range of their targets:

> In my day to day life, I find myself hacking everything imaginable. I hack traffic lights, pay phones, answering machines, micro-wave ovens, VCR's, you name it, without even thinking twice. To me hacking is just changing the conditions over and over again until there's a different response. In today's mechanical world, the opportunities for this kind of experimentation are endless (Kane 1989: pp 67-69).

Dutch hackers Gongrijp and Dell in relating some of their activities illustrated how broadly the desire to technologically explore can reach. Dell claimed to have physically explored the subterranean tunnels and elevator shafts of Amsterdam including government nuclear fall-out shelters. Gongrijp described how he had

entered the out-of-bounds areas of buildings such as banks by pretending to accompany legitimate tour groups and then taking the first opportunity to wander off on his own, assessing the security of the site and then somewhat cheekily informing the security staff of that assessment (Gongrijp: Amsterdam interview). The "technology" which is the subject of their curiosity in these cases, simply being the architecture and security features of buildings which they found interesting.

The heterogenous range of technological targets considered as "hackable" is described by Ralph, a Dutch hacker, who argued that hacking is not just about computer break-ins but should be defined so that it does not:

> only pertain to computers but pertains to any field of technology. Like, if you haven't got a kettle to boil water with and you use your coffee machine to boil water with, then that in my mind is a hack. Because you're using the technology in a way that it's not supposed to be used. Now that also pertains to telephones, if you're going to use your telephone to do various things that aren't supposed to be done with a telephone, then that's a hack. If you are going to use your skills as a car mechanic to make your motor do things it's not supposed to be doing, then that's a hack. So, for me it's not only computers it's anything varying from locks, computers, telephones, magnetic cards, you name it (Ralph: Utrecht interview).

Gongrijp described, as his example of the heterogeneity of hacking, how, "the Wageningen agricultural university a couple of years ago had a couple of students doing a project enhancing the genes of marijuana plants, to me that's gene-hacking, it's more than science, it's just somebody gets a kick out of it". He argued that hacking is a frame of mind, a sort of intellectual curiosity that attaches itself to more than just one type of technology or technological artefact: " ... for me a hacker is more all-round than to some people, I think a hacker is not a real hacker unless he has a basis in two or three skills, not just hacking Unix systems but also a

little bit of something else, electronics, audio hacking or something general" (Amsterdam interview). This heterogeneity of hacking's targets fuels the 'kick' gained from satisfying the primary urge of technological curiosity:

> in the early days of say the uses of electricity and how to generate it, were first developed, I think Tesla and all the people who were playing with it then were as much hackers as most computer hackers are now, they are playing on the frontier of technology and all those hefty experiments were not only done for science, they were done because they got a kick out of it (Gongrijp: Amsterdam interview).

The 'kick', thus gained, crucially depends upon an element of inventiveness which serves to distinguish 'true hacks' from those that could be labelled as acts of 'Nintendo Perseverance', that is, hacks which exhibit large amounts of concentration and dedication rather than ingenuity. Methods of hacking entry may become widely publicised by means of the various branches of the hacker grape-vine, for example, electronic and paper-based specialist magazines, or even "word of electronic-mouth". From such sources, hacking 'cook-books' result. Those that predominantly, or exclusively, use such sources of information for the illicit use of a technology, can be technically labelled as hackers since they fulfil the definition's basic property of the illicit use of a technology. However, the Dutch hackers I spoke with were keen to differentiate themselves from such people, by imparting their concept of a hack similar to Turkle's description of the Holy-Grail type hack.

Using the example of phone phreaking phone-calls Ralph illustrates this distinction between a technical and a 'true hack':

> it depends on how you do it, the thing is that you've got your guys that think up these things, they consider the technological elements of a phone-booth, and they think, "hey, wait a minute, if I do this, this could work", so as an experiment, they cut the wire and it works, now THEY'RE hackers. Okay, so it's been published, so Joe Bloggs reads this and says, "hey, great, I have

to phone my folks up in Australia", so he goes out, cuts the wire, makes phone calls, leaves it regardless. He's a stupid ignoramous, yeah?

The second situation is another hacker reads this and thinks, "hey, this is an idea, let's expand on this". So what he does is go to a phone box, he cuts the wire, puts a magnetic switch inbetween, puts the magnetic switch up against the case, closes the door again and whenever he wants to make a free phone call, he puts a magnet on top, makes the wires disconnect, and he has a free phone call, goes away, takes the magnet away and everybody else has to pay. Now he's more of a hacker straight away, it's not a simple black and white thing (Ralph: Utrecht interview).

Thus it is evident that there are various forms a hack can take, and a hacker tends to be defined not just by what he does but by how he does it. A 'true' hack should involve an element of originality in keeping with the characteristic typical of the hacking fraternity of this study, namely the way their mind perceives unorthodox ways of subverting any given technical situation. For example, Gongrijp pointed out in an Amsterdam housing estate, startlingly vivid yellow paint on road over-pass supports. He explained that it was indelible anti-graffiti paint and observed wryly that people could cause havoc if they used such paint for graffiti purposes (Gongrijp: Amsterdam interview).

4.1.2 The hacker ethic

Fuelling the hack and setting the ideal standard of hacking morality within the culture of hacking is the ethos of the early MIT hackers. Its main tenet was, according to Levy:

> Access to computers - and anything which might teach you something about the way the world works - should be unlimited and total. Always yield to the Hands-On imperative! [Levy, 1984:40].

More specific elements of this hacker ethic consist of the following points:

1. "All information should be free".

2. "Mistrust Authority- Promote Decentralisation".

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

4. "You can create art and beauty on a computer".

5. "Computers can change your life for the better".

(Levy 1984: pp 40-45).

Bill Landreth also describes the intended ethical outlook of a hacker group he was instrumental in setting up in 1982. They called themselves the "Inner Circle", an elite group of hackers who could trade information amongst themselves and thereby avoid passing on information to less ethical hackers liable to use it for nefarious ends. The need for such a group had arisen due to the huge increase in the amount of hackers at this time, itself attributable to the increased diffusion of microcomputers. Typically for hackers and the informal nature of their culture, whilst claiming to be an ethical group, no attempt was made to formally draw up a specific code of behaviour. If such an attempt had been made, Landreth argues, it would have been as follows:

> No Inner Circle member will ever delete or damage information that belongs to a legitimate user of the system in any way that the member cannot easily correct himself. No member will leave another hacker's name or phone number on any computer system. He will leave his own on a system only at his own risk. All members are expected to obtain and contribute their own account information, rather than use only

information given to them by other members (Landreth 1985: pp18-19).

The most important underlying principle behind this purported code of behaviour, Landreth contends, was respect for other people's property and information: "We were explorers, not spies, and to us, damaging computer files was not only clumsy and inelegant - it was wrong". Having described how hacking involved its own particular ethic and 'kick' we now turn to a more detailed exploration of its culture.

4.2 HACKING CULTURE

> *It's Sunday night, and I'm in my room, deep into a hack. My eyes are on the monitor, and my hands are on the keyboard, but my mind is really on the operating system of a superminicomputer a thousand miles away ... The only light in the room comes from the green screen of my computer monitor and the small red lights on my modem. I turn and check the clock: 3:00 a.m. "Good," I think. "Three hours before I have to leave for school. Too bad I didn't have time to do any homework." Thoughts of school evaporate, and I return to my computer with the enthusiasm of a Super Bowl football player* (Landreth 1985: 57).

This section examines the social element of hacking that such a portrayal would seem to leave little room for. It is difficult, however, to readily identify an obviously structured group acting as a CU culture in an open way. The 'culture' of the CU is mediated by the fact that it 'inhabits' a non-traditional environment which has the inherent quality of anonymity and invisibility: a basic lack of physicality:

> To find 'Hacker Culture' you have to take a very wide view of the cyberspace terrain and watch the interactions among physically diversified people who have in common a mania for machines and software. What you will find will be a gossamer

framework of culture. Come back in 100 years and you may see more (Marotta: e-mail interview).

A comprehensive description of the social organisation of hackers has been attempted by Gordon Meyer (1989). The limited scope of the work, however, means that scant attention is paid to the actual culture of that social organisation. It is the 'gossamer framework of culture' that this section explores, starting with its two primary underpinning aspects: the hack and the hacker ethic. From these fundamental elements of hacking has sprung what is difficult to define unequivocally, but what is generally recognised as a hacking culture:

> Cultures have (1) Technology (2) Institutions (3) Language (4) Arts. By this measure, what is 'Catholic Culture'? It is heavy on Institution and weak on Technology. Hacker culture is obviously very technological. Hacker Language is based on jargon that separates it from mainstream English. Hacker Arts would be centred on Star Trek and fractals. But you would be hard-pressed to find a reason for saying that Classical or Electronic New Age Music is 'hacker' since some probably enjoy Rap far more (Mercury: e-mail).

This description illustrates the difficulties faced when trying to define 'hacking culture'. The following section discusses the elements that are relatively easy to identify.

4.2.1 Hacking Culture - Specific elements

(i) Technology content

Hacking culture is epitomised by its easy relationship with technology. For the first time, a new generation of young people are growing up completely at home with computers and their capabilities:

> What we are confronted with is a generation that has lived with computers virtually from the cradle, and therefore have

> no trace of fear, not even a trace of reverence. To me, a computer is still, well, something to be revered. When I started my career in computing, there wasn't really computing at that time ... there were about three of them, you had one shot at a run a day if you were lucky. It was sacrosanct, it no longer is to those kids, you go in, have a bash at the keyboard, they're convinced by experience that nothing much can go wrong (Herschberg: Delft interview).

We will see throughout this study that technology inevitably forms the material basis of hacking culture. We have already seen how a crucial element of hacking resides in the innate curiosity with which hackers approach a diverse range of technological artefacts. Such a quality has existed throughout history, but the mass diffusion of computing and telecommunication equipment has meant that curiosity can more easily utilise technological artefacts for purposes, or by people, not originally intended in the initial design of the objects. The significance of hacking's technology-based culture is that it represents a qualitatively new challenge to governments and establishment forces who may no longer have a monopoly power over the ways in which technology is controlled and used. It raises questions concerning the nature of ownership in an era of 'informational plenty', and the possibility of adequate government or societal control over the new communication technologies. The key political aspect of hacking rests with the fact that it represents a direct challenge to government control of technology of a more worrying kind than previously arising with the perennial presence of innovative and curious individuals. The advent of the 'cyberspace' and advanced telecommunication systems has created the conditions necessary for cooperation between previously geographically dispersed and hence isolated, technologically curious people.

(ii) Secrecy

Another characteristic of hacking is its secrecy. This causes obvious difficulties for any attempt at describing its culture, for example its true size is largely unknown:

> Some professional informants ... have estimated the hacker population as high as fifty thousand. This is likely highly inflated, unless one counts every single teenage software pirate and petty phone-booth thief. My best guess is about five thousand people. Of these, I would guess that as few as a hundred are truly 'elite' - active computer intruders, skilled enough to penetrate sophisticated systems and truly to worry computer security and law enforcement (Sterling 1992: 77).

The following description given by Schifreen helps to account for many of the difficulties in drawing a detailed picture of hacking culture. He described the immediate impact on his local hacking group when he related how recent legislation appeared to have forced hackers underground:

> There used to be a hacking community in the UK, the hackers I used to deal with 8 or 9 years ago, where all based in North London where I used to live and there were 12 of us around the table at the local Chinese restaurant of a Friday night, talking about lots of things and getting through lots of Diet Coke ... within about 20 minutes of me and my colleague Steve Gold being arrested: end of hacking community. An awful lot of phone calls went round, a lot of discs got buried in the garden, and a lot of people became ex-hackers and there's really no-one who'll talk now, it's difficult (Schifreen: London Interview).

The following is an example of the enforced atmosphere of secrecy within hacking circles that makes identification of any overt cultural qualities, difficult. Mofo was a hacker encountered in the e-mail fieldwork who was using somebody else's account and the above pseudonym as a precaution against identification. He asked

me to: "Tell me more about yourself, but wait about a week to respond as I use this account only with the 'permission' of the real owner and login only occasionally. I login on this account very infrequently as I do not want to get the rightful owner any undue attention" (Mofo: e-mail interview). He proceeded to describe in the following manner, his views and interpretation of the significance of the actions of Robert Morris[3]. The quotation below is illuminating in the way it vividly portrays how hackers in the CU depend upon secrecy, and trust each other not to act in any way which might incur a clampdown from the law-enforcement agencies, fear of whom increasingly characterises part of the CU milieu:

> BTW, I think that you might be interested to know that I and many others have used the UNIX sendmail bug to access many, many systems throughout the world (without damaging data in any way) until that stupendous asshole, Robert Morris, royally phucked everything up for us. I've known about the print f () sendmail bug ever since I got access to source. Only a dummy would publicize something as good as that by doing something completely phucking stoopid like what Morris did. His idiocy cost hackers/phreakers more than anyone can imagine (Mofo: e-mail interview).

The Robert Morris incident seemed to mark a watershed in the openness of the Internet. During the late 1980's and early 1990's there was a series of 'crackdowns' in the form of legislation and arrests by Secret Services/Police forces[4]. Sources, such as the Computer Underground Digest, have repeatedly drawn attention to the belief, commonly held within the underground community, that the establishment has been guilty of paranoia and over-reaction in their pursuit of hackers. The commonly portrayed image is that of secret service men raiding adolescent, bespectacled hackers' homes

---

[3] The Internet Worm was a worm program written by Robert Morris Jr., ironically the son of the National Computer Security Centre's chief scientist. It hit the Internet network of computers on November 2nd 1988, estimates of affected machines range from 6,200 to 2,000.

[4] c.f. The Hacker Crackdown by Bruce Sterling, in which he documents and comments upon the spate of U.S. Secret Service investigations into CU activity in the early 1990's.

with guns drawn. Such operations are known as 'stings' and have such colourful names as 'Operation Sun Devil'. The establishment's reaction also takes less dramatic forms. I was informed by a Dutch programmer that one of the Dutch hackers interviewed as part of this study was under surveillance by the security services, and Schifreen describes how he came to give up hacking after having had his equipment seized by the police at the start of their investigations into his hacking activity: "When I got it back, I'd sort of lost the inclination and I was sort of scared as well, because when you're on bail, it's not a good idea to carry on doing it. Plus the fact that it's pretty certain that my phone was being tapped" (Schifreen: London interview).

(iii) Anonymity

Cyberspace's ultra-modern, 'virtual' depiction of increasing immateriality questions some of our notions of what constitutes reality and threatens some conventional notions based upon physical reality. It can also, however, be conceptualised as a reinforcement of reality in the sense that:

> In many ways, the world of cyberspace is more real than the real world itself. I say this because it is only within the virtual world that people are really free to be themselves - to speak without fear of reprisal, to be anonymous if they so choose, to participate in a dialogue where one is judged by the merits of their words, not the colour of their skin or the timbre of their voice. Contrast this to the 'real' world where we often have people sized up before they even utter a word (Goldstein: CuD 5.43).

Part of the hacker ethic as described by Levy is the assertion that "Hackers should be judged by their hacking, not by bogus criteria such as degrees, age, race, or position". The egalitarianism of such a principle within the hacker culture is aided by the fact that

computer communication is intrinsically non-physical[5], as a result, computer communication generally fails to differentiate between normal social hierarchies.

> power and prestige are communicated neither contextually (the way secretaries and meeting rooms and clothes communicate) nor dynamically (the way gaze, touch, and facial and paralinguistic behaviour communicate; Edinger and Patterson, 1983). Thus charismatic and high status people may have less influence, and group members may participate more equally in computer communication (Dunlop 1992:334).

Stemming from the disembodied characteristics of computer mediated communication (CMC), e-mail correspondence generally has a depersonalised quality, the reception of an e-mail message occurs without any accompanying indicators. Even with non-interactive and inanimate means of communication as traditional letters, important information can be transmitted from aspects such as the letterhead. E-mail, in contrast, is blind as to the social position or mood of the sender, which would normally be conveyed by facial expressions and general demeanour.

One result of this blindness is the tendency of many e-mailers to drop some of the conventions and propriety that are normally expected in more traditional forms of communication. 'Flaming', is a term used to describe the particularly vituperative tirades of insults which can result when an e-mail discussion or disagreement becomes heated. The experience of the French introduction of the minitel chat system[6], is one risque and vivid illustration of the way in which the status-stripping qualities of e-mail can reduce people's expressive inhibitions. People seem to have a somewhat surprisingly ready predisposition to swap intimate details of each other's lives, more

---

[5]For example, to compensate for the inability of computer communication to convey certain gestures and emotions, users have developed various computer substitutes. During my research I came across the following examples: [; -)] to express a winking face, that is, irony or sarcasm; [: - 0] to express shock;
[: -)] happiness, and so on.

[6] c.f. De Lacy, Justine "The Sexy Computer" (1989)

specifically, their sex lives and accompanying fantasies, a

phenomenon which seems to be exacerbated by the fact, peculiar to e-mail correspondence, that those communicating have no visual or aural clues as to the identity of their correspondent.

The hacking community and its accompanying culture is directly affected by such qualities of CMC. The anonymity it produces means that 'exploration' by hackers is not of a direct physical nature, and this may play a role in hackers being slow in many cases to accept responsibility for their actions, or that their actions are in any way morally wrong. CMC qualities, as will be shown later, also have important effects upon the nature of the establishment's response to the computer underground and its activity, tending to exacerbate fears of it and increase its underground status.

(iv) Fluidity of boundaries and speed of change

The third quality of hacking culture relates to the fluidity of its boundaries and the speed with which it changes. Clough and Mungo described how, from the point of view of law enforcement, the computer underground represents an amorphous, constantly changing environment:

> There is no organized structure in the computer underworld, no mysterious chairman of the board to run things. The underground is anarchic, a confederation of phreakers/hackers and virus writers from all over the world whose common interests transcend culture or language. Most hackers have two or three handles and operate on a number of boards. They change ID's, aliases, sites, their methods, targets and gang membership as rapidly as the authorities track them. Stamping out hacking is like trying to pin down mercury (Clough and Mungo 1992:18).

In addition to the intrinsic intangibility of groups existing by means of CMC, the medium also encourages a constantly shifting environment:

People come and go pretty often, and if you lay off for a few months and then come back, almost everyone is new. There are always those who have been around for years, but you can weed out the amateurs by comparing two lists of names acquired several months apart from each other ... I would consider the hacker community a very informal one. It is pretty much anarchy as far as rule-making goes. The hacker ethic is not always applied, unfortunately, (and that's why hacking has such a bad name). The community was structured only within the framework of different hacking "groups". Legion of Doom would be one example of this. A group creates its own rules, and usually doesn't have a leader ... The groups I've been in have voted on accepting new members, kicking people out, etc (Eric Coggans: e-mail interview).

4.2.2 Hacking and gender: male predominance

A hallmark of the event [Hack-Tic computer club's 1993 Summer Conference] was the male to female ratio: running at roughly 100:1, it did not bode well for the demise of the anorak. Even so there was some emergence of a hacker chic, with one of the few women sporting jewellery made from watch parts and hair decoration courtesy of an eviscerated floppy disk (Goodwins 1993: 11).

Faced with the above difficulties of establishing a coherent hacker culture, one characteristic of it that does stand out is the male dominance of the activity. This section looks at the possible reasons for hacking's gender bias, and thereby introduces the whole general issue of what factors motivate hacking:

The computer underworld is populated with young men (and almost no women) who live out their fantasies of power and glory on a keyboard. Most are single. That some young men find computing a substitute for sexual activity is probably incontrovertible. Just as a handle will often hide a shy and frightened fifteen-year-old, an obsession with computing to the exclusion of all else may represent security for a sexually insecure youngster. The computer is his partner, his handle is

> his real self ... and the virus he writes is the child of his real self and his partner. A German virus writer once said: "You feel something wonderful has happened when you've produced one. You've created something which lives. You don't know where it will go or what it will do, but you know it will live on." He was talking about his new virus (Clough and Mungo 1992:8).

The above quotation is one sexually-based theory of why, as is generally accepted, there are almost no female hackers active in the computer underground. The research failed to uncover any significant evidence of females active in hacker-related fields, and as can be seen from the quantitative survey, only 3% of respondents to a questionnaire, widely dispersed throughout the computing community, were female. Examples of women, active in or at least associated with related activities, are: Susan Thunder, an associate of Kevin Mitnick, described in Cyberpunk; during an American radio phone-in programme on hacking[7], a woman called Anna proclaimed herself to be a phone-phreak; and in Approaching Zero the authors describe how "Leslie Lynne Doucette was once described as the 'female Fagin' of the computer underworld. In her mid-thirties, she was considerably older than the 150 or so adolescent Olivers she gathered into her ring. As a woman, she has the distinction of being one of only two or three female hackers who have ever come to the attention of the authorities." (Clough and Mungo 1992:148). Keller states that:

> In the course of a career in computing which spans 20 years in industry and academia in the United States and Great Britain I have met several people I would call *hackers* ... I have never met a female hacker. No one I know with whom I have discussed hacking can recall an instance of meeting or hearing of a female hacker...[and in a footnote] ... The Hacker's Handbook, 3rd Edition mentions one, but at one point puts *she* in quotes, as though to denote irony or uncertainty about that particular hacker's true gender (Keller 1988: 57).

---

[7] Ed Schwartz Show on WGN Radio. September, 27-28, 1988.
Transcript published in Phrack Vol 2, Iss 21.

Although computing still tends to be a male-dominated environment, the almost complete absence of identifiable female hackers does not seem to be adequately explained by merely drawing attention to the minority status of women in computing. There are still sufficient numbers of women in computing to suggest that statistically one would expect the existence of some female hackers. Ellen Spertus in her paper, "Why are There are so Few Female Computer Scientists?" states that "In the most recent years for which figures are available, women received a third of the bachelor's degrees in computer science [in the USA], 27% of master's degrees, and 13% of PhDs." (Spertus 1991: i) These figures would lead one to expect the existence of at least some female hackers, but such hackers do not seem to be forthcoming. No women hackers were in fact encountered in direct fieldwork or in the "snowballing" technique used in the electronic-mail interviewing as described in the methodology chapter. The question of why, therefore, there is such a dearth of female hackers will be looked at directly in the next section, whilst the peculiarly masculine aspects of hacking will be further illustrated throughout the study in subsequent sections analysing the culture of hacking.

4.2.3 Reasons for the paucity of female hackers

Spertus looks at factors that discourage women from computer science in general, rather than the act of hacking, specifically, the factors relating to the former, however, are also relevant to the latter. Her three main reason why women are discouraged from computer science are:

1. Societal factors - e.g. the sexual stereotyping of young children, the boys are given technical toys. The girls are given cuddly toys.
2. The masculine environment - computer science is dominated by men and therefore this creates a general 'locker-room' climate in which women feel threatened or uncomfortable.

3. Gender in language - the male gender-bias in the language used in computer science reinforces points 1 and 2.

(i) Societal factors

Sherry Turkle emphasises the differences of approach to computing that gender seems to produce are culturally reinforced. She argues that males tend to exhibit tendencies towards 'hard mastery' and females tend towards 'soft mastery': "Hard mastery is the imposition of will over the machine through the implementation of a plan ... Soft mastery is more interactive ... try this, wait for a response, try something else, let the overall shape emerge from interaction with the medium. It is more like a conversation than a monologue" (Turkle 1984: pp 102-3). Whilst men tend to be overwhelmingly 'hard masters' females are generally 'soft masters'. This would be an immediate reason why females tend to be excluded from the 'hard' world of hacking and a general fascination for technology and what it can do:

> In our culture girls are taught the characteristics of soft mastery - negotiation, compromise, give-and-take - as psychological virtues, while models of male behaviour stress decisiveness and the imposition of will ... Scientific objects are placed in a "space" psychologically far away from the world of everyday life, from the world of emotions and relationships. Men seem able, willing and invested in constructing these separate "objective" worlds, which they can visit as neutral observers ... We can see why women might experience a conflict between this construction of science and what feels like "their way" of dealing with the world, a way that leaves more room for continuous relationships between the self and other (Turkle 1984:107 +115).

Hacking does seem to convey a feeling of power which arguably appeals to the male gender more than the female:

> The deep attraction of this sensation of elite technical power should never be underestimated. "Technical power" is not for everybody; for many people, it has no charm at all. But for some people, it becomes the core of their lives. For a few it is overwhelming, obsessive; it becomes something close to an addiction. People - especially clever teenage boys whose lives are otherwise mostly powerless and put-upon - love this sensation of secret power and are willing to do all sorts of amazing things to achieve it (Sterling 1993:19).

The qualitative field-work responses pointed to a general uncertainty or lack of conclusive arguments for the general absence of female computer scientists or hackers. They tended to emphasise the societal argument factors in preference to the other potential reasons of a threatening, biased-language environment. Several e-mail correspondents identified general social trends discouraging women from scientific pursuits such as computing. Social factors seem to be mixed in equal part with tentative views that women are psychologically less amenable to the 'hard mastery' implicit within computing. Krista Bradford, a female American journalist who has had an interest in computing for 10 years, argued:

> I think you have to go back to the day women are born and the kind of social conditioning we get ... I believe the culture discourages women from pursuing math/science. The computing process/logic seems much more 'male' to me personally - more linear than circular thought (somehow my Macintosh seems friendlier and therefore more 'female') ... more Spock than Captain Kirk (Bradford: e-mail interview).

Whilst Mercury contended:

> When Adam delved and Eve span ... who was then the gentleman? Well, we see that Adam delves into the workings of computers and networks and meanwhile Eve spins, what? Programs? again, my wife programs and she has the skills of a hacker. She has had to crack security in order to do her job. But she does it AS HER JOB, not for the abstract thrill of

> discovering the unknown. Eve spins. Females who compute would rather spend their time BUILDING a GOOD system, than breaking into someone else's system (Mercury: e-mail interview).

Jean-Bernard Condat, President of the French Computer Chaos Club, gives a perspective which fuels some of the suspicions that hackers may have a sexist streak:

> In France, the boys play computers and bicycles and/or skate-board, and the girls are at home. Technology is for a long time in my country an uni-sexual one. The notion of male/female criteria is not an important one. It's the cognitive aspects of the hacker ... and a tradition factor. The long concentration of the hacker's spirit on a particular problem is, perhaps, possible only for French boys! (Condat: e-mail interview).

A different emphasis was placed upon the potential psychological differences between men and women by a security manager, Bob Johnson:

> Most men see a problem or puzzle as a direct challenge. They keep attacking it until it's solved, and then brag about it. Women will fuss with a problem for a little while, decide it's too hard, and will drop it. I've heard about experiments where students were given puzzles with varying degrees of difficulty, including some that were unsolveable. Men tended to keep fighting with the unsolveable puzzles and get quite frustrated and angry. Most women simply gave up. In discussing this question, I got some other thought-provoking questions. How come you don't see women working for hours on puzzles like the Rubik's cube? How come you don't see women sitting in front of a Nintendo game for days on end? How come there are many more men in prisons than women? Psychological make-up? Ethics? Sociological pressures? Peer pressure? Different maturity levels? Western cultural roles? Who knows?!? (Johnson: e-mail interview).

The research found no evidence which conclusively refutes the notion that there may be some innate gender differences in the responses of men and women to computing and so they remain a possible explanation. There is evidence both from the literature and fieldwork, however, of identifiable social trends that discourage the women from computing.

Factors (ii) and (iii) the masculine environment and gender in language: cybersexism?

It would seem that males involved in computing are more predisposed to enjoy the anonymity and lack of personal contact afforded by electronic-mail, than are their female counterparts. The 'maleness' of the cyberspace environment is reinforced by its frontier-like status vividly described by John Perry Barlow (1990). Such a frontier-like status also has the effect of encouraging and emphasising the penchant adolescent males seem to have for exploration, be it physical space or increasingly computer cyberspace: "But then teen-age boys have been proceeding uninvited since the dawn of human puberty. It seems hard-wired. The only innovation is in the new form of the forbidden zone and the means of getting in it" (Barlow 1990: 48).

Barlow, compares cyberspace to the "Wild West", and draws attention to the machismo nature of hackers: "the actual natives are solitary and independent, sometimes to the point of sociopathy. It is of course a perfect breeding ground for outlaws and new ideas about liberty" (ibid: 45). He communicated with various hackers during an on-line conference, his initial sympathy for crackers diminished "under a steady barrage of typed testosterone" (ibid: 46), a machismo that is exaggerated by the nature of the medium within which they 'electronically travel'.

Within the male-dominated world of computing there are accusations of blatant anti-female sentiments . In an article printed in the Computer Underground Digest and entitled "Sexism and the CU" Liz E. Borden writes:

> skewed participation transports the male culture of values, language, concerns, and actions, into a new world and creates models that women must conform to or be excluded from full membership ... BBSs, especially those catering to adolescents and college students, are frightening in their misogyny ... sexism is rampant on the nets. The alt.sex (bondage, gifs, what-have-you) appeal to male fantasies of a type that degrades women (Cud 3:00, article 4).

In the ensuing debate that this posting gave rise to, a man replied that the misogyny in the CU is:

> a sad reflection of how our society has created values by way of mass media ... First, when measured against the standards of today's society, "six foot, 180 lbs of tanned muscle, a full head of perfect hair, and gorgeous eyes," few computer freaks measure up. preferring the "safeness" of their computers ... Computers don't turn you down for a date. As a result, a growing misogyny appears and manifests itself through computers where the individual can remain basically formless through either pseudonyms, or just the relative anonymity that comes from no-one knowing what they "look like". (Brain Scott Wilson: CuD #3:01).

Martin Freiss, a German hacker, concurred with this assessment of the role anonymity plays in increasing misogny in computing:

> What often happens when a female appears on the network is that the male majority "jumps" on her. The fact that many networks allow a user to hide his real name, i.e. cloak a user in anonymity, seems to cause many males to drop all semblance of civilization. Sexual harassment by e-mail is not uncommon, both in universities and commercial institutions [not excluding the company I work for] (E-mail interview).

The world of computing may be also be less appealing to women as a result of the fact that their small numerical presence produces the 'threatening situation' of disproportionate interest and

friendliness from the male computer scientists keen to meet a female peer. Thus 'Mercury' relates how, "My wife runs a couple of AT&T 3B2s and so she belongs to a UNIX user group. She never lacks for attention when she goes to meetings! So you can't say that hackers are 'anti-female'. (Mercury:e-mail interview)

However, the loosening of sexual mores and inhibitions afforded by the anonymity of the Internet is thus seen as producing the threatening and unattractive situation that women wishing to participate in the computer underground have complained about. An illustration of this atmosphere is provided by a poem, published without any accompanying criticism in CuD:

DOES SHE DO THE VULCAN MIND MELD ON THE FIRST DATE?

By Nick Herbert. From MONDO 2000, the magazine for cyberspace.

"I want your bra size, baby,
Fax number, E-mail address,
Modem com code, ID,
Phone machine access.

Give me you thumb print, password,
Blood type and credit check;
Give me your anti-body spectrum,
Your immune response spec.

Let's break bread together baby,
Exchange cryptographic primes;
Let's link up our parallel ports;
And go on-line in real-time.

Let's indulge in covalent bondage;
Let's communicate in C.
Let's merge our enemy bodies
And bob in the quantum sea.

I wanna swim in your gene pool, mama;
Snort your pheromones up close range;
Tune in your neurotransmitters,
Introduce you to Doctor Strange.

I wanna surf in your quantum potentia;
Mess with your thermostat;
Wanna tour your molecular orbits;
Wanna feed your Schrodinger cat.

Let's surgically merge our organs;
Our kidneys, our lungs and our hearts;
Let's read our physics journals together
And laugh at the dirty parts.

Let's Bell-connect our bellies
With some quantum-adhesive glue;
Let's do new stuff to each other
That Newton never knew.

I wanna feel your viscosity, honey,
Melt my rheological mind;
Let your female force-field vortex
Deform my male spacetime." (CuD#4:17)

(iv) Hacking and the role of sexuality

John Perry Barlow (1990) described the motivations of hackers as, "exploration and thrill-seeking. Young men are hard-wired with an urge to violate the forbidden. Over the millenia, they've found numerous surrogates for the "real thing" they're most motivated to violate, computers only being the most recent". A spokesman for a group calling themselves "Toxic Shock" seems to add weight to any Freudian-based theories that hackers may hack in order to fulfil some deep-rooted desire to penetrate and violate, with his 'orgasmic' description of hacking:

> It doesn't happen like Wargames shows it. Oh no, it is so much different. The geek in the movie ... he had it so easy. No real hackers would exist if it was that easy (perhaps therein lies the solution to the "problem"). No, we hack and hack at a system like a man on safari, clearing away the vines of the jungle with his machete, trying to forge ahead to a destination he cannot yet see. We keep on, torturing our brains and pounding our fingers on the keyboard until at last ... oh at long, sweet last ... we are in (Toxic Shock- CuD 2:06).

Keller further explores the sexually-based motivational explanation of hacking initiated by "Toxic Shock": "In the sense that hacking is a solitary and non-constructive activity, it might be termed *masturbatory*. The pleasure or interest is confined to the activity itself, and has no object, such as a lover, and no objective, such as a demonstration of affection" (Keller 1988: 57).

(v) Hacking and machismo

Reflecting some of the above perceptions that hacking may be motivated by gender and sexual factors, Keller (1990) explains hacking as a manifestation of machismo: "hacking is an aberrant behaviour related to *machismo* ... *Machismo* is an exaggerated form of male posturing designed to demonstrate a high degree of masculinity through the accomplishment of acts of proof, with the object of exciting the admiration of others and (perhaps also) demonstrating contempt for the less masculine" (Keller 1990: 58). Using this definition of machismo to explain and conceptualise the activity of hacking is problematic, however. For example, Keller attempts to argue that hackers succumb to the macho vice of only enjoying glory which accrues to the individual and is unshared. She compares hacking to bull-running at Pamplona and argues that, "It is necessary to act alone, to dare the bull as an individual, without the help of others. As I have observed, the hacker is also solitary." (*ibid*: 59) Two of the Dutch groups interviewed, however, seemed to have a closely-knit collective approach to their hacking activities, each hacker tending to have their own delineated areas of specialism which contribute to the overall group effort. For this limited sample of groups at least, there did not seem to be an innate need to appropriate individual glory. Keller also claims that hackers, in a fashion similar to that seen with serial killers, generally seek recognition of their cleverness from such establishment figures as the law enforcement people out to catch them.

Gongrijp and Ralph, however, both argued that the most accomplished hackers are those whose exploits are least known. The hackers who are most publicised tend to be those who have been caught through technical carelessness and are sneered at by others in the hacking community for such carelessness. From the sample of hackers interviewed, (especially the "Zoetermeer Gang"), the desire to receive recognition seemed to be limited to their immediate peer group of hackers. It has already been noted that the hackers interviewed were self-selecting in that they were willing to talk in the first place. They were therefore interested, to some extent at least, in receiving recognition for their activities. Although it is difficult to gauge objectively, the extent to which their willingness to talk about their hacking may have been due to this desire, they did not seem to suffer from a disproportionate tendency towards publicity-seeking. Rather there seemed to be amongst them a wish to rectify the situation whereby their abiding interest of hacking had received scant academic or rigorous non-sensationalised reporting.

4.3 ACADEMIC MOTIVATION THEORIES

Given that hackers are predominantly male and that this fact may be due to a combination of social and psycho-sexual reasons, the issue remains as to why hackers male or otherwise hack at all:

> There are a lot of people interested in playing around at hacking out of sheer curiosity and a small group whose interest is motivated out of mischief and malevolence. There's a macho prowess to hacking, it's a challenge. (Dr Peter Ross, Deputy Head of Edinburgh University's Artificial Intelligence Dept.: Student Thurs 25th Feb, pg 1).

As the above quotation illustrates, there are various and sometimes interrelated explanations of what motivates hackers to hack. Two academics who have theorised about the possible psychological motivations of hacking are Joseph Weizenbaum (1976) and Sherry Turkle (1984). Both highlight the perception that

hacking is the preserve of compulsive computer programmers lacking social skills.

For example, Weizenbaum's portrayal of the act of hacking provides a seminal description of its obsessional elements:

> Wherever computer centres have become established ... bright young men of disheveled appearance, often with sunken glowing eyes, can be seen sitting at computer consoles, their arms tensed, and waiting to fire, their fingers, already poised to strike at the buttons and keys on which their attention seems to be as riveted as a gambler's on the rolling dice. When not so transfixed they often sit at tables strewn with computer print-outs over which they pore like possessed students of a cabalistic text (Weizenbaum 1976: 125).

Turkle also concentrates upon hackers as those programmers who love the computing machine for itself, as an end in itself, rather than as a tool, as a means to an end. Her analysis is a powerful inquiry into the nature of compulsive programming and extreme psychological identification with the computer as a type of emotional mirror or even soul-mate. The motivation of the compulsive programmer derives from the wish to escape from the contingencies of the real world by revelling in the hygienic safety offered by the computer.

Turkle and Weizenbaum's concentration upon compulsive programming emphasises how it is often pursued at the expense of the ability to conduct "normal" social relations. The stereotypical "computer geek" therefore, is someone who finds refuge from what seems to be a hostile world in the safety of a computing environment. Thus Turkle describes, in language similar to that used by Shallis in The Silicon Idol, how, "Like Narcissus and his reflection, people who work with computers can easily fall in love with the worlds they have constructed or with their performances in the worlds created for them by others. Involvement with simulated worlds affects relationships with the real one" (Turkle 1984:78).

Turkle describes case studies of various personality types that use the computer as a psychological refuge in this way. There is a danger, however, that such work leads to a tendency for all hackers, or anyone deeply enthusiastic about computing, to be predefined as compulsively or addictively involved in computing to the detriment of social relations. Whilst computing, along with lots of other activities, may have its element of compulsive afficionadoes, the research suggests that hacking and computer addiction are not mutually inclusive. Shotton (1989), for example, focuses upon the personalities of 'computer dependents' who may or may not be hackers, but whom are characterised by the disproportionate amount of time they devote to computing. She concludes that portrayals of computer enthusiasts as socially inadequate addicts is inaccurate:

> Early readings about 'computer junkies' and 'hackers' suggested that if I pursued this research I might spend my time with people who were barely human and who were unable to converse with others on any meaningful level. How untrue this proved to be. I met some of the most fascinating people of my life. They were intelligent, lively, amusing, original, inventive and very hospitable...They were pursuing an interest which not only provided intellectual challenge, fun and excitement in infinite variety, but one which enabled many of them to improve their career prospects considerably. Many used computers not only at home but also at work, and true fulfilment must come to those who are able to combine their hobby with a means of earning a living (Shotton 1989: Preface).

Turkle is eventually forced to recognise that hacking is not reducible to compulsive programming. Thus she describes the concept of "the hack" and separates it from her discussion of computer addiction: a step that Weizenbaum eschews. Models of people using computers for psycho-sexual reasons of dependence or insecurity may give an accurate description of some compulsive programmers but they are lacking as a full explanation of the causes and implications of the type of hacking encountered in this study, the defining quality of which is the desire to achieve a hack.

4.4 HACKERS' DESCRIPTIONS OF WHY THEY HACK.

Having established what it is to hack, there follow excerpts from members of the hacking community describing the particular reasons why they hack. They show how hackers perceive themselves and their social position, as opposed to the interpretations of 'outside groups'. The CSI, for example, are accused of emphasising the vandal-orientated motivations and pathological psychological aspects of hacking. The limitation of a purely psychological approach are outlined below by a hacker, 'Mofo the Clown'. He emphasises the distinction to be made between a hacker and a 'vandal':

> 'Hacker' to me is a term which defines an individual who succumbs to his/her thirst for knowledge (and the computing power that accompanies that knowledge). A 'hacker' will not ever maliciously commit or condone and action of destruction (be it physical or electronic) of computers or data. A vandal rejoices in his/her ability to wreak havoc upon systems run by ignorant individuals. Most often such a vandal will not seek to maintain accessibility to systems that he/she has compromised. Instead, seeking to destroy data or make life generally more difficult for users and administrators. Vandals feel the need for power as manifested in the microcosm of the machine (Mofo: e-mail interview).

In the course of this study the following main motivations for hacking were encountered:

1. Feelings of Addiction.
2. The urge of curiosity.
3. Boredom with educational system.
4. Enjoyment of feelings of power.
5. Peer Recognition.

Turkle, Shotton and Weizenbaum, as we have seen, have addressed category 1, whilst Keller alone has briefly treated category 5. The other categories have been largely ignored, a gap this study's fieldwork evidence seeks to fill.

4.4.1 FEELINGS OF ADDICTION

(i) Fieldwork evidence

Evidence of the compulsive behaviour the academic literature identifies is also apparent from the hackers themselves:

> Damn kid. All he does is play games. They're all alike. And then it happened ... a door opened to a world ... rushing through the phone line like heroin through an addicts veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought ... a board is found. "This is it...this is where I belong (The "Mentor". Phrack - Vol 1 Iss 7).

> We are addicted to information and knowledge, and our drugs are withheld from us. We are forced to seek our precious information and knowledge elsewhere. We have to find challenge somewhere, somehow, or it tears our very souls apart. And we are, eventually, forced to enter someone's system (The Toxic Shock Group CuD no. 2.06).

Addictive affinity with computers is illustrated often by the choice of words hackers use to express themselves. President of the French Computer Chaos Club, Jean-Paul Condat:

> All the hackers that I know in France, have (or have had serious problems with their parents. Some speak only by computer or only the computer matters. Hacking for a real hacker is the only reason to live! Without background ideas. Like drinking water for a human body. The lack of computers/software to hack make the hacker ill at ease (Condat: e-mail interview).

Maelstrom described his urge to hack in terms which in addition to making use of addictive imagery also lend weight to Turkle's theory that hackers may use the computer as some sort of psychological prop:

> I just do it because it makes me feel good, as in better than anything else that I've ever experienced. Computers are the only thing that have ever given me this feeling ... the adrenaline rush I get when I'm trying to evade authority, the thrill I get from having written a program that does something that was supposed to be impossible to do, and the ability to have social relations with other hackers are all very addictive. I get depressed when I'm away from a networked computer for too long. I find conversations held in cyberspace much more meaningful and enjoyable than conversing with people in physical-reality real mode. For a long time, I was extremely shy around others, and I am able to let my thoughts run free when I am alone with my computer and a modem hooked up to it. I consider myself addicted to hacking. If I were ever in a position where I knew my computer activity was over with for the rest of my life, I would suffer withdrawal. (Maelstrom: e-mail interview).

The addictive aspects of hacking, however, only partially describe an activity that has an array of intermingled motivations. Feelings of addiction are not the sine qua non of the activity. Johnson, approached the question of compulsion by making a distinction between intellectual curiosity and compulsion with the use of an analogy:

> An automobile mechanic when fixing a motor should find the problem, replace broken parts, and complete the job. If he indulged his intellectual curiosity, he might take apart some of the motor, in order to see how it works ... If the mechanic tears the motor completely apart, or goes home and spends every waking moment tearing down and rebuilding car motors, then his behaviour has become compulsive. Will it make him a better mechanic in the long run? Probably, if he doesn't burn out (or his wife doesn't kill him). If he starts sneaking into his

neighbour's garage at midnight to "work on" his neighbour's BMW, something's dreadfully wrong (Johnson: e-mail interview).

Johnson makes the point that compulsion does not have to necessarily equate with hacking. The compulsion that **some** hackers show causes a mystique around hacking simply because computers appear to the public as more mysterious and esoteric than other technological artefacts with which they have more knowledge and everyday contact. The 'wizard-like' and addictive images of hackers portrayed in popular representations of their activity may therefore lessen as computers becomes less novel and more widely integrated into society:

> We have seen the same kind of compulsive curiosity with Nintendo video game systems here in the States. Kids will literally spend days playing a single game, until they master it. There is nothing inherently compulsive in computers, any more than in booze, drugs, television, food, work, art or anything else. Compulsive behaviour is found in people, not in things. A person can be compulsive about anything. It's just more interesting when a person is compulsive about computers, than if they're compulsive about clothes or cars. Hackers are not necessarily compulsive. Computer addicts are not necessarily hackers (Johnson: e-mail interview).

Hacking, therefore, does not have to have predominantly negative effects upon its practitioners, and it is perhaps unfair to attribute to computers qualities of addiction, whilst similar behaviour would not be so described in relation to other activities. In so far as computer/hacking addiction would imply a reduced ability to socially interact, at least those hackers interviewed seemed to belie the stereotype of the hacker as the computer geek. Several of the hackers interviewed had started their own computer security businesses with an entrepreneurial zeal that sits uncomfortably with the image of reclusive 'computer geeks'.

John Butler (Edinburgh University computing officer), provided his own interpretation of some of the reasons why hacking may become compulsive or addictive. He related how some course administrators had asked him to deny internet access to certain students because they had become "NewsNet Junkies". His observation was that computing offers "an alternative reality and there's a disconnection between it and the real world" (Butler: Edinburgh interview). This disconnection can then prove to be a source of hacking addiction since hackers working for many long hours in such an "alternate reality", may begin to have increasing difficulty distinguishing between their reality and the real world.

A specific reason why hackers may be viewed as compulsive by outsiders to their "alternative world" was described by Mike who argued that the speed of change of the computing environment, identified earlier as a distinctive part of hacking culture, means that they have to approach their past-time with above average application:

> No, it's not compulsive, but if you stop, if you don't do it for one week then things change, the network always changes. It changes very quickly and you have to keep up and you have to learn all the tricks by heart, the default passwords, the bugs you need. If you want to get into a system you have to try anything, so you have to know every bug (Utrecht interview).

Hackers, therefore, have an immediate tendency to involve themselves with their alternative reality to a greater extent than that contemplated by more 'nine-to-five-minded' computer people.

(ii) <u>The Bedworth case</u>

"COMPUTERS TURNED MY BOY INTO A ROBOT" -Daily Mirror headline Mar 18th, 1993.

Below is the Independent newspaper's editorial response to the most recent significant hacking incident: the prosecution of an Edinburgh University Student, Paul Bedworth, the first prosecution under the 1990 Computer Misuse Act. The case ended in an acquittal on March 17th, 1993:

> It was agreed that Mr Bedworth had broken into numerous computers in Britain and abroad by calling from the BBC microcomputer in his bedroom; that he had changed the data inside those computers; and that he had made more than 50,000 calls for which he had not paid. But his counsel found an expert witness to convince the jury that the hacker had no intent to commit the crimes, because he was so addicted to his computer that he was no longer responsible for his actions (The Independent: Thurs, March 1993).

This case is the best example to date of the issue of addiction and hacking. It also returns us to some of the issues discussed in Chapter 3 regarding the potentially dehumanising effects of computer technology. Bedworth's barrister, Mr Alistair Kelman argued that: "Mr Bedworth was ... someone who had grown up with computers and been damaged by them. 'When a kid's best friend becomes a computer rather than a member of their family then you are courting trouble' " (Independent March 1993). The extent of this trouble is illustrated in the following description:

> Paul Bedworth is small and slightly built but he was strong enough to push his mother down a flight of attic stairs when she tried to stop him using his computer ... So great was Paul's obsession that the only way Mrs Bedworth could force him to take a break was by switching off the electricity supply at the mains ... Only sheer exhaustion would force Paul to stop. His mother would find him slumped across the keyboard or face down on the carpet where he had collapsed. 'It was so worrying because he would be lying there with his nose in the carpet looking like he had fainted or was dead' (Scotsman 18.3.1993: pg 3).

Professor Griffith-Edwards from the Addiction Research Unit in London, was called as an expert witness. His description of Bedworth was, "One is looking at a young man with monstrously abnormal behaviour. I would classify him as suffering from a mental disorder, as distinct from a mental illness, but a very serious one" (The Scotsman 18.3.1993: pg 3). The response to the Bedworth case, although predominantly emphasising his obsessional nature also added weight to Johnson's assessment of compulsive hacking being a particular example of a single-mindedness apparent in various otherwise harmless endeavours. Prof Osborne from Swansea University Psychology dept, consulted after the verdict argued that: "Computer addicts may sit in their bedroom for long hours but I am not sure there is any different personality trait here than in a compulsive gardener", whilst Shotton, replying to the accusation that hackers tend to be disproportionately introverted, makes the point that: "This is quite normal behaviour. Not all people are gregarious and raving extroverts. Heaven help the world if everyone was" (The Times 18.3.1993: pg 5). Furthermore, the intellectual aspects of hacking mean that it is more likely to be excusable as a type of commendable attempt to exercise the mind, than it is to be condemned as a solitary obsessive waste of time.

4.4.2 Curiosity - humans and technology

> *What a hacker does primarily is relentlessly pursue an answer. Computers naturally lend themselves to this sort of pursuit, since they tend to be patient when asked a lot of questions* (Goldstein: CuD 5.43).

Hackers emphasise the innate curiosity with which all human beings approach technology and from which technological improvements and adaptations are ultimately derived. The 'hacker mentality' therefore is seen as a positive attribute which drives forward technological development. The fact that hacker culture is

replete with artefacts, results in hackers having more opportunities to indulge their curiosity:

> Oppression is our only reward ... yet if it were not for people like us, all of you who wake up each day to an alarm clock, or drive to work in your fine new car after cutting on your security system, while drinking that cup of coffee you didn't have to get up to prepare, would still be living in a cave, somewhere near Africa, grunting and reproducing, eating the raw meat of some beast you hunted down with clubs, trying to ignore the cold that seeps in through the animal skins you wear, and wondering why some curious person with some intelligence, creativity, and ingenuity would come along and invent the wheel (Toxic shock 1990).

4.4.3 Boredom aspects

In contrast to, and as a result of, the hacker penchant for exploration is a low threshold of boredom for computing activities not of their own choosing. One of the most common complaints I encountered when talking with hackers was that they were bored with the computing education they received in a formal learning setting such as university or college. The following quotation illustrates the depth of feeling of hackers have concerning the extent to which they feel orthodox education methods have failed to address their needs:

> we've been spoon-fed baby food at school when we hungered for steak ... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert (The "Mentor". Phrack - Vol 1 Iss 7).

The quotation vividly portray the hacker argument that boredom with the educational system is a contributing factor to their activity. Related to these feelings of being educationally circumscribed are those which result from i) lack of mental

stimulation in computing courses. ii) inadequate access to computing facilities.

(i) Lack of mental stimulation

Examples of the views articulated in the above quotation abound in the fieldwork. Thom Van Os and the Zoetermeer group of hackers claimed to be signally underchallenged by their assignments at university. For others, once their boredom is removed and they are given responsibility, the urge to crack may stop. John Draper claimed that this was his experience when he was made the manager of a system used by students, whom he found himself disciplining and discouraging from destructive acts. The experience of 'Faustus' seems to verify the idea that removing boredom from the minds of hackers means that their abilities can be more productively utilised. He relates how:

> kids are bored and feel powerless in a system run by often unfriendly adults, and cracking is their only way to assert themselves. Very often a clever cracker is made into a system manager, and this is a good way to make him stop cracking, since once he is "part of the system", the frustration that is the reason for attacking it disappears. When I was a kid (i.e. 16-18) I spent some time trying to crack systems, but nothing serious. I quickly became a "manager type" and haven't had any motivation since then to mess with security (Faustus: e-mail interview).

Thus added responsibility may limit the need to hack but may still not satisfy the illicit thrill associated with unauthorised intrusions. J.C. Van Winkel a software engineer and researcher who has worked in various "tiger teams", and has been used to test the security of various sites relates how:

> I did hacking because for me it was a way to learn more about the system, curiosity and not anything else, I wanted to learn more about it and they didn't give me enough information. I

> mean I was pretty good at that time, I got high grades and didn't have to do anything about it, so I was bored if I didn't do anything and together with a couple of colleagues we wrote programs that were far from what the normal scientists wrote ... I think a lot of it's boredom and people like to have puzzles, I mean why do people do crosswords?... it's the same thing with hackers ...We took the most difficult assignments because we liked to do it, on the other hand, curiosity will never be satisfied (J.C. Van Winkel: Appledorn interview).

There is perhaps the intractable problem, that whereas hackers seem to need their curiosity and intellects satisfied, it is likely that for some people at least such curiosity is insatiable.

(ii) Lack of access

A common complaint encountered in the research from hackers and dovish elements of the CSI, was that hacking is exacerbated due to hackers lack of access to computing facilities:

> It is my contention that if Robert Morris had a legitimate venue for exploration, he would not have launched a virus on the Internet. If the Dark Avenger (who wrote a virus of the same name) had been given some guidance, he would not have launched the virus (I have met him and am now convinced that he is being turned 'to the good side' by several caring people who saw his plight and are spending the necessary time with him). I know that many of the 'hackers' I knew when I was younger would gladly have done their work with permission, but the paranoia and maniacal attitudes of those in the computing community prevented the legitimate exercise of their interests (Dr Cohen: e-mail interview).

The specific experience of Brian Thompsett, a Computer Science Lecturer at Hull University (formerly of Edinburgh University), further illustrates the complaint regarding adequate access to facilities. He experienced what he perceived to be a limitation of access to computing facilities from Edinburgh University Computing

Service (EUCS). The dispute centred on whether his work fulfiled the EUCS regulation of computing access only being given to those whose requirements satisfied the criteria of "reasonable usage", after a drawn-out dispute Thompsett was given a machine to do with as he pleased, he further related how:

> Now I had the computer I began to realise that I wasn't the only victim of the strange rules on computer usage. I decided to run the donated machine on a laissez-faire basis. This is working well. The basis of the arrangement is that people can explore computers on my machine. It acts as a honey-pot principle. If we let them burn out their nasty tendencies in my sand-pit then they leave the rest of the EUCS machines alone. If they mess around in the sand pit the other kids push them out. Works so far. So it boils down to this. I have a machine on which lots of users might be considered 'naughty boys' elsewhere, but on my machine they get to play without monster nanny breathing down their neck. They manage to mature quite nicely in a year or so. Some of my kiddies have now evolved into quite responsible people. Several important machines in the U.K. are now managed by some people in my user community (Thompsett: e-mail interview).

Thompsett's open-access machine became known as 'The Tardis', privileged users/supervisors becoming known as 'Time Lords', one of whom, Malcom Campbell (Edinburgh interview), concurred with Thompsett's opinion that the project helps to mature computer users that might otherwise turn to electronic vandalism. The argument, similar to those used in 'real world' acts of vandalism, contends that users who have a stake in the 'system' are unlikely to jeopardise their user rights. The sanction of exclusion from the Tardis system proved to be an effective deterrent for would-be malicious hackers.

Another area of complaint is that even when courses do stimulate they are accompanied by a lack of access to systems. This lack of access is compounded by a lack of university courses for those hackers too young to attend, yet sometimes extremely able.

The contention is that a lack of access to mailing facilities and the internet news etc. is a major cause of hacking. A contributing factor is the cost of using various systems.

Critics of hacking would question the right of hackers to make use of other people's telecommunication systems without paying for the privilege. The hackers interviewed, however, claimed that they had no ethical qualms in using facilities they would not otherwise be able to afford and that the nature of communication technologies is such that the marginally increased use of the system by hackers, does not lead to increased prices for other consumers. Maelstrom applied this argument to both communication systems and software copyright protection:

> I've learnt a bit about the Unix and VMS operating systems, have made many friends via TALK and PHONE utilities, and now know a lot more about computer security than I ever thought I would. I will have no moral or ethical qualms whatsoever about system hacking until accounts are available to the general public for free. MSU's $460 per year charge for an internet connection for telenetting just doesn't cut it for a high school or college student who is strapped for cash ... For a computer enthusiast to go by the law would be to spend hundreds of dollars per month on programs and various accounts on systems. Hacking will always exist in some form or another until a person can do things without losing his shirt (Maelstrom: e-mail interview).

James Carlson, involved in commercial computing, does regard most underground activities as due to a lack of access to adequate facilities:

> Nearly all are benign. I did some of this kind of hacking myself when I was in high school. I think I did it mainly because there were few facilities available for my use ... and the only ones that were available (at school) were highly restricted ... How about just providing better facilities and access for new users? Why can't ALL people get electronic- mail? Why can't everyone have access to open systems? These things would

provide a more-than-necessary distraction for the average hacker (Carlson: e-mail interview).

Coggans, in addition, argues:

> If people were given legitimate access to the systems they wanted to learn about, and were given the ability to send mail and communicate with each other interactively, much of the hacking would subside. Having a legal internet account is what has saved me. I can still blab with my peers on IRC, I can send mail to everyone, and I can snoop around via FTP completely legally on a UNIX VMS or NOS! That in addition to the systems I am given limited permission to access via clients contracts, my needs are fulfilled completely, and I have no desire to access systems which are forbidden to me. I think if people were given this type of arrangement early on, it would curb the urge to break into other sites (Coggans: e-mail interview).

Rop Gongrijp, further argued that the technical knowledge of increasingly young hackers sits ill with the lack of opportunity that those young hackers have to exercise that knowledge. They are aware of the internet, which will not be accessible to them until they are 19-20:

> I mean I know a few kids that I associate with, they have no option, they are 14, they can't wait, what do I tell them? "Well, just be good for a while, put up with the fact that they have nothing but boring assignments for you, and it'll be five years before you have any assignments at all ... And then in five years you might be able to work in a completely censored environment ... Am I supposed to say that to 14 year olds that want to explore? Great prospect, so I tell them, go ahead, hack, don't break anything but explore what you want to explore, grab your computer and modem and see what's out there, I mean if that takes breaking into systems that they don't want you into for the next five years, do it. I think there is a moral right for that kid to go out and explore keeping people away from technology or anything that long does not work (Gongrijp: Amsterdam interview).

4.4.4 Enjoyment of feelings of power

> *Becoming computer literate, comments Paul Kalaghan, dean of computer science at Northeastern University, 'is a chance to spend your life working with devices smarter than you are, and yet have control over them. It's like carrying a six-gun on the old frontier (Roszak '86: 67)*

Linked to the previously mentioned notion of machismo in hacking culture is the motivational factor of power. Journalistic investigations of hacking have tended to concentrate on the "power" element behind hacking activity. Without doubt, however, feelings of power do complement the main motivation of curiosity, in Beating the System Edward Singh is reported as confessing that:

> Part of it was a sense of power. You were running an informal network of about 250 computers and no-one else outside your close circle of friends knew about it. The final goal was total world domination, to have everything under control. It was the ultimate game on the ultimate scale. You got a thrill out of knowing how much power you had. It was possibly hitting back at society. There was a sort of political anarchism involved. The main thrill was beating the system (Bowcott and Hamilton 1990:42).

From Singh's rather dramatic analysis of his own actions Bowcott and Hamilton derived the title for their book on hacking. Immediately after the above 'confession', however, they admit that on another occasion Singh accounted for his actions as being primarily motivated by intellectual enjoyment. To a limited extent, there was acceptance of the concept of power as a motivating factor by the hackers interviewed. Thus Thom Van Os of the "Zoetermeer gang" of hackers commented, "Most of the hackers do it for the kicks, I suppose. Breaking into a bigger or more important system, or acquiring root-status can give you a real feeling of power and you

seem to have proved yourself better than the system administrator" (Zoetermeer interview).

In the unusual interviewing situation referred to in the methodology chapter, the issue of power as a possible motivation of hacking was raised with Kevin Mitnick: 'the dark-side hacker' portrayed as determined to make nefarious use of the power computers offered over other people. Mitnick denied the suggestion that he was ever motivated by any sinister factors such as strong yearnings of power, but recognised that some hacking is carried out for criminal gain. Instead, he hacked because:

> You get a better understanding of the cyberspace, the computer systems, the operating systems, how the computer systems interact with one another, that basically, was my motivation behind my hacking activity in the past, it was just from the gain of knowledge and the thrill of adventure, nothing that was well and truly sinister such as trying to get any type of monetary gain or anything (Mitnick: telephone interview, Holland - USA).

Another example of hackers deriving what could be labelled as a hypothetical, as opposed to a malevolent sense of power, is their collection of potentially destructive information for the simple act of collection rather than any particular use to which it could be put. Hack-Tic shares with such publications as Phrack and TAP, the characteristic of containing much esoteric, yet potentially dangerous information. Thus throughout issues of Phrack are instructions on how to make various explosives such as Nitro-Gylcerine. To most people outside the hacking world, such information and its promulgation would seem, at best, of dubious value and, at worst, extremely irresponsible. The fact that hackers spread, but would be extremely unlikely to use such knowledge for any concrete purpose, is indicative of their general ethos that purports information to be of value or interest in its own right. This may partially explain the fact that much hacking activity does not seem to have any "useful" eventual purpose. The activity is an end in itself and the intellectual

exercise of gaining knowledge is its own justification. Rop explains this tendency of his magazine and those like Phrack of disseminating diverse forms of technological knowledge irrespective of the possible uses or value of that information, as follows:

> the information is out there and the people who are going to make bombs have the information anyway, if you want to make a bomb you can get all the information on how to build a nuclear bomb if you want to, you just look in the library, and it's just that so many people enjoy reading about something they will never do just for the sake of reading about it. I mean if I publish a scheme on how to rob ATM's (automatic telling machines) and I make the scheme real elaborate, where it takes video cameras and organisation, nobody's probably going to do that except the people that already knew how to do that anyway. It's only for the sense of adventure of the people that read that and think "wow! this is great: a sense of power" (Gongrijp: Amsterdam interview).

The informational content of such magazines as Hack-Tic, however, can be of practical use. It is generally concerned with electronic gadgetry and 'blue-box technology' for phreaking free phone calls. The magazine has, for example, gained some notoriety by giving details of how to make free phone calls from public pay-phones, and this has called into question some of the above claims of the disinterested publication of information.

4.4.5 Peer recognition and hacking culture

The final motivational category is that of a sense of peer recognition. One example of an individual looking for recognition outside of a group of hackers is that provided by the account of Gerry Santoro from Penn State University:

> About two years ago a teaching assistant (T.A.) for my Computing in the Humanities class figured out the password for one of my mainframe disks. He then proceeded to copy files from me, including a file that listed all students and their

passwords. When the T.A. was caught he denied having done this, claiming that he didn't know how he got the files. At the same time, other members of the student computing community reported that he was bragging about how he had 'outsmarted' the computer center and that no files were safe from his intrusion if he desired. I believe this particular student did if for the peer-group status that it afforded. This particular student did not have much of a social life outside of classes, and therefore this was a realistic route for obtaining (in his mind) a positive self-image (Santoro e-mail interview).

Hackers themselves admit to this element of peer-encouraged behaviour. Maelstrom admitted that:

> Peer recognition was very important, when you were recognised, you had access to more. For instance, on chat systems where private channels could be set up and people could only enter by invitation, you had to be known and respected before you got to join the discussion. Also, many people hacked for fame as well as the rush. Anyone who gets an informative article in a magazine (i.e. Phrack, NIA, etc) can be admitted to bulletin boards. Finding new user passwords requires only a few contacts, and contacts can be found on chat systems (even public non-hacker ones) (Maelstrom e-mail interview).

Direct personal experience of such peer recognition was hard to gain from the fieldwork because interviews, with the exception of the Zoetermeer group and the hackers at the headquarters of Hack-Tic, were only carried out on a one to one basis. This largely precluded the possibility of gauging the extent to which status amongst their peers motivates hackers to hack. The Zoetermeer group's activity was largely based upon their university contact with each other, and their individual hacking was encouraged by there being a receptive audience amongst both an inner and outer group of admirers:

> Hacking can be rewarding in itself, because it can give you a real kick sometimes. But it can give you a lot more satisfaction and recognition if you can share your experiences with others. Next to that it is very useful if you operate in a group, because many know more than one alone. I think the group nature is important because of the recognition you can get from the group; doing bigger and better hacks clearly distinguishes you from other people. Here at my school the group nature is also very important in providing a competitive environment which proves very motivating. Without this group I would never have spent so much time behind the terminals digging into the operating system. Our group consists of a core of about 6/7 people and lots of people hanging around (in blind admiration ;-)) (Zoetermeer interview).

4.5 CONCLUSION

The analysis of hacking culture prepares the ground for the explanation contained within the subsequent chapters of the process by which society responds to hacking. Having given a full account of the nature of the CU, it is then possible to evaluate more accurately the conditions that allow hacking to continue; the extent to which it is of potential benefit or poses a threat to the computing industry; and the likely success and implications of measures taken to eliminate it. This chapter's portrayal of hacking culture was predominantly based upon hackers' own descriptions of their milieu, added to which are the identifiable elements of the culture encountered during the course of the fieldwork. This 'internalist' account of hacking can be compared later in the study to the various ways in which groups outside of hacking perceive the activity: the 'externalist account'. It is the conflict between the two perceptions that gives rise to the process of closure.

The chapter identifies various elements of hacking culture. Building a definitive picture of such a culture, however, is inherently unachievable. The CU presents itself as a 'gossamer framework' of contacts and communication networks, the insubstantiality of which is exacerbated by computer networking's anonymous qualities. It is

further heightened by the climate of secrecy resulting from the fear and suspicion that arose after various legal crackdowns on hacking.

In conjunction with the additional motivational categories of addiction and power-seeking, this chapter has expanded upon the issues raised in Chapter 3 regarding the nature of the relationship between human beings and technology. The implications of the relationship are ambivalent. It forms both a rebuttal to, and confirmation of, concerns that technology dominates people instead of vice versa. Hackers reject technological domination to the extent that they revel in any opportunities they find to demonstrate their power to control computer systems; yet they also reinforce concerns of technological determinism in the instances where they epitomise addictive reliance on artefacts. Apart from the strength with which hackers such as Maelstrom express their feelings and their accompanying use of addictive language, their statements are interesting for the emphasis they give to the social aspects of hacking. Hacking on the one hand has qualities symptomatic of an addictive pastime, with all the accompanying connotations of enervation, and yet at the same time, it can actually be a positive influence on developing more sociable personality traits, as shown by Maelstrom's account of how he feels much less shy and inhibited conversing by computer than he does in 'physical reality mode'. The common depiction of hackers as people who have personality difficulties due to their obsessive use of computers may therefore be too simplistic. Hacking may attract a disproportionate amount of people with a predisposition to shyness and a lack of social skills. The overall effect of hacking upon such people, instead of exacerbating such traits, may in fact counter them.

Despite the various weaknesses of the 'Machismo model', the evidence does suggest that deep-rooted gender differences account for the overwhelming predominance of men as opposed to women who exhibit "Nintendo perseverance" and the destructive tendencies of some virus-writers. The reason why gender differences still persist in less destructive areas of hacking is more likely to be due to societal factors which, in turn, are more liable to be eventually

rectified to produce conditions more favourable to increased female participation. The extent to which such psychological factors as those identified by Turkle persist, will obviously limit the extent to which improvements in these conditions can be made.

The preponderance of men in hacking implies the dominance of 'hard' mastery over its more feminine 'soft' counterpart. The fact that hard mastery relies heavily upon objectivity and instrumental reasoning would seem to reduce the alternative culture status of hacking, since these two qualities are aspects of technological usage that are typically criticised in calls for technologies that embody more humane values. The danger of some computer users exhibiting addictive tendencies towards their activity also undermines arguments for hacking's technologically liberating potential.

It is important to have a balanced understanding of what motivates hacking, especially if policies are to be developed with which to tap it, channel it in other directions, or to reduce it. The thorough examination of motivations in this chapter, has demonstrated that there is a complex mix of factors underpinning hacking, although many of these tend to be ignored by the academic studies that emphasise its more obsessional aspects. The fact that the factors motivating hacking are frequently intermingled complicates the task facing policies aimed at combatting hacking. For example, one of the apparent causes of the activity, is the coexistence of hackers' intelligence with what they perceive to be the boredom of an educational environment that fails to stimulate. A logical response aimed at limiting the incidence of hacking, therefore, would be to increase the interest quotient of the courses. However, even if this could be achieved, the illicit thrill of exercising anti-bureaucratic power would still make it likely that hacking would continue to some extent. The evidence would thus seem to predict that no one solution aimed at eliminating hacking will succeed in addressing the mix of possible motivations that fuel the act.

Chapter 5 - State of the industry: hawks and doves

5.1 INTRODUCTION

5.2 THE EXISTENCE OF SECURITY WEAKNESSES
5.2.1 Qualitative evidence
5.2.2 Statistical evidence
5.2.3 Quantitative questionaire data

5.3 REASONS FOR SECURITY FLAWS
5.3.1 The Software Crisis
5.3.2 The Software crisis and the origins of hacking
5.3.3 The problem of anticipation and the role of testing
5.3.4 The knowledge gap
5.3.5 Commercial pressures and security holes

5.4 THE RATIONALE FOR HACKERS

5.5 RATIONALE FOR NON-COOPERATON 'THE HAWKS'

5.6 CONCLUSION

5.1 INTRODUCTION

This chapter examines the state of security within computing and why it has weaknesses that allow hackers to access other peoples' computer systems. It analyses the problems of adequately structuring programs associated with the 'software crisis' and how those problems are reflected in both the earliest and current forms of hacking. The chapter outlines the extent to which security flaws exist; the reasons they are not eliminated; and the potential role hackers might have as correctors of such faults.

From both the quantitative and qualitative fieldwork, there was a general consensus of opinion from the CSI and CU that there are large and continuing security faults in many systems. The reasons given for such flaws are both technical and commercial: computer systems are intrinsically insecure in the sense that they cannot be guaranteed, a priori, to be totally impervious to intrusion; commercial pressures are such that there is a tendency to skimp on the security measures and procedures that do exist; and similarly, education about computer security suffers from a low profile in both the academic and business sectors.

Once it has been established that there is a fundamental need for security improvements within computing, the chapter looks at hackers' claims that they have real technical knowledge that could be used to provide them. The question then arises as to why cooperation between the CSI and the CU does not occur on a larger scale and why hackers do not now have the level of acceptance enjoyed in their early MIT days. Chapter Six describes how the first hackers were largely tolerated because their knowledge was valued and useful despite its often unusual methods of acquistion. What was once tolerated in the academic pursuit of knowledge, however, is no longer tolerable in the increasingly commercial environment of computing, the changing nature of which has led to a hardening of attitudes towards hackers. As a result the CU's expertise in security is not generally utilised by the CSI. Generally poor quality of security

within computing coexists with the potential for technical fixes from the hacking community. This leads to the assumption that hackers are being marginalised away from a core of influence within computing and that this is due primarily to social rather than technical reasons: an example of a technology's development being caused by a deliberate process of social shaping. This chapter therefore provides the initial evidence for the argument that a process of closure and stabilisation has occurred within computing.

The chapter also adds to the description of the constituency of computing initiated in the previous chapter, by describing the nature of the computer security 'industry' and the way in which their external view of hacking compares with the hackers' internalist account. The previous analysis of the hacking community has illustrated the way in which it defines itself and how elements of its behaviour may set it apart from other members of the computing community. Culture formation is an on-going process and the delineation of boundaries between the CU and the rest of computing depends upon this active differentiation from others. Elements of the CSI wholeheartedly oppose hacking and its purported ethic, and the subsequent exercise of closure whereby it undertakes to isolate the CU is also part of the process by which the CSI promotes its own identity.

This identity, however, is not unequivocally established. In contrast, to the amorphous nature of the CU, the CSI consists of those who live in the institutional worlds of business or academia. Although the CSI therefore has more of an institutional setting, it too lacks an identifiable culture in the sense that it has no official professional structure. People gain a reputation as computer professionals with security expertise, expertise often gained on an ad hoc basis. The term 'CSI' is thus used guardedly, there are, for example, various figures that have changed their nominal group status: previous members of the CU are now involved in the provision of security services, a phenomenon characterised as 'the poacher-turned-game-keeper' scenario, and academics such as Herschberg straddle both main groups. Within the CSI itself, there

are two broad, conflicting strands of opinion regarding hacking: the 'hawks' and the 'doves'. As the two phrases imply, the former strongly oppose hackers whilst the latter advocate listening to their views and in some cases actively cooperating with them in order to improve computer security. These two groups are two extremes of a spectrum of opinion with regard to hackers. The rationale behind both their views is explored in preparation for the next chapter's analysis of the specific processes by which the CSI forms its opinions about hackers.

5.2 THE EXISTENCE OF SECURITY WEAKNESSES

5.2.1 Qualitative evidence

The hackers interviewed related their experiences of their unauthorised intrusions into computer systems. Their accounts illustrated computing's poor state of security. In addition, the general impression encountered in the fieldwork from members of the CSI was one of resignation as to the continued future likelihood of serious security breaches:

> I have been in more systems than one can imagine, ranging from military installations, financial installations, to soda companies. I have seen insider-trading information, had access to transferrable funds, had the ability to manipulate credit information and have had complete control over phone networks (Chris Coggans: e-mail interview).

> I obtained a whole slew of accounts on Eastern Michigan University's VAX/VMS system. I've also gotten into very critical test-creation accounts at colleges and unversities. It's amazing how easy it often is to get into important accounts that many instructors access (Maelstrom: e-mail interview).

The fact that computer systems are vulnerable to attack is ironically underlined by the fact that hackers have been criticised for seldom, if ever, making use of original, previously unknown security

weaknesses. The incident of the Internet Worm, for example, was often referred to as 'an accident waiting to happen'. To compound matters, even when specific technical fixes have been produced for some of the threats posed by hackers, the incremental nature of much software development is such that hackers can make use, not only of technical weaknesses in systems, but also the logistical problems encountered in attempting to fix them:

> Hackers rarely exploit the full spectrum of IT risks! Apart from a few instances, such as worm technology and stealth viruses), hackers actually use rather primitive methods to access systems, program and data. E.g. the NASA hack exploited a hole in a DEC VMS version when this hole was in prinicipal already patched; while DEC customers had received (and hopefully installed) the patch when the attack was undertaken, the hackers used a second-hand system (not bought directly from DEC) whose existence was not known to DEC, and where the patch was not sent! (Brunnstein: e-mail interview).

Coggans illustrates the relative ease with which unauthorised access can be gained to computer systems. In his description of several of his break-ins, he claims to have seen:

> The advertising campaign outlines for 'new' Coke months before its release; insider stock trading information in mail on Citibank computers, electronic fund transfer systems; military systems with 'sensitive' non-classified information, phone company computers that allow you to listen in on any telephone call in that area; credit computers; the ministry of treasury system in South Africa (whose MOTD [Message Of The Day] changed to "end apartheid now" as if by magic) (Coggans: e-mail interview).

Maelstrom and Coggans also both described the way in which their phone-phreaking activities combined with their computing knowledge to enable them to enjoy unbilled international

teleconferencing, in addition to the ability to eavesdrop at will on other peoples' telephone calls. Maelstrom recounted how he:

> learnt to use the Michigan C/NA (Customer Name and Address) bureau, which allowed me to dial up a computer and, after entering a passcode, use touch tones to get information on the owner of any Michigan telephone number. Some of my friends from around the world would start AT&T Alliance teleconferences every so often, and we would talk throughout the night, sometimes for as long as 12 hours at a shot (which was probably not good for grades at school). On one memorable conference Cellular Phantom demonstrated a REMOB number (REMote OBservation) which allowed us to listen in on any phone line in the country at will ... I learned quite a bit about how much privacy people REALLY have as opposed to what they THINK they have ... (Maelstrom: e-mail interview).

Whilst Coggans argues that:

> I know all too well how simple it is to view and alter consumer credit, to transfer funds, to monitor telephone conversations etc. ... I can monitor data on any network in existence, I can obtain root priveleges on ANY Sun Microsystems UNIX. If I, a 22 year-old, non-degreed, self-taught individual can do these things, what can a professionally taught, profit motivated individual do? THERE IS NO PRIVACY ... People need to know the truth about the vulnerabilities of the computers they have entrusted their lives to (Coggans: e-mail interview).

The vulnerability of computer systems to intrusions was also recognised by members of the CSI. Their resultant concerns about the potential of hacking to cause damage fuels the sense of antipathy that exists between the CSI and the CU.

> Maybe I'm a bit old-fashioned but in my mind once a criminal, always a criminal ... I reject utterly the idea that they browse, I reject utterly and completely that because I don't believe they know. Many installations wouldn't know because they don't

> keep that type of record ... there's lots of crashes in many systems ... further over in North Wales, they had a system crash, they never found out why that system crashed, I made several suggestions as to why it had crashed, they didn't want to know. I reckon the DP manager knew damn well what had happened, somebody had mucked about with the software (Tozer: Hawarden interview).

A similar, but more conclusive, experience was recounted by a computer security officer from a U.S. military site, Thomas Zmudzinski:

> Back in 1989, another nearby facility was penetrated, and the intruder gained control of an industrial process. The product of this process is so specialized that there is no other source. Fortunately, it was local enough that we could trace him. He was still playing with his new 'toy' when the police broke down his parents' (!) door. The raw materials he used were worth more than one million U.S. dollars, and everyone involved thought it was a minor miracle that he hadn't destroyed the plant! [It really happened, I was there, believe it!] (Zmudzinski: e-mail interview).

To add to the alleged vulnerability of systems to outsiders is the added danger of hacking from insiders intimate with the working details of particular systems. The view that concern over the vulnerability of systems to outside intrusion generally fails to take into account intrusions from people working inside systems, was underlined by several interviewees who asked to remain anonymous because they did not want their employers to become aware of the fact that they hacked. The point that familiarity with a system increases the potential for unauthorised use and hence increases the vulnerability of a system to 'internal hacking' would seem to be underlined by Appendix 1's statistical data.

An illustration of the vulnerability of systems is the generic nature of hacking. That is, often the ability to hacking into one computer system can be applied to a whole class of systems.

Herschberg pointed out that when he accepts a documented hack as a Masters' Thesis, the penetration described within the thesis should be for a class of systems as opposed to just one individual system: "it's always a class ... hack one, hack all, otherwise it doesn't count, proper penetration is generic" (Herschberg: Delft interview). This generic nature of hacking, however, also causes great concern for the CSI due to the resultant failure of distance to contribute to a system's security. Once a flaw has been found in a system it is then vulnerable not just to local hackers, but the world-wide community. Coggans related how: "today hackers have everything documented for them on the usage of a plethora of systems by past hackers". (Coggans: e-mail interview). Holbrook explains why this situation can cause concern about security threats to assume paranoid proportions:

> I would go back to the analogy about physical tresspass. In that realm, the amount of damage that an intruder can use is usually related to how much effort they put in, how much expertise they have, and so forth. People are very comfortable with what kinds of threats exist in the 'real world' and how to deal with them. There is no similar comfort level in the computer world. With the breakdown of physical barriers surrounding computers that the network brings, organisations have equal risk from malicious local users and from crackers half way around the world. Intruders can compromise and damage a system with information that could be found on a cracker bbs. Most computer systems don't have any levels of security. Any gap is sufficient to compromise the entire system. So some paranoia is warranted! (Holbrook: e-mail interview).

The generic quality of hacking, in addition, may exacerbate the vulnerability of systems to damaging security breaches, over and above, the deliberate damage of malicious hackers because of the tendency of non-malicious but careless system intruders to inadvertantly cause damage. Coggans relates:

> In my own experience, I was VERY cautious in the early days. I didn't just barge in to a system like the stereotypical 'bull in a china shop' and I imagine most people keep this level of alertness. Even with this heightened sensitivity to the potential disasters, some people still executed programs they shouldn't have, edited sensitive data, etc ... Today it seems many hackers just don't care, but then again, today hackers have everything documented for them on the usage of a plethora of systems by past hackers, so perhaps armed with these instructions they feel overly confident from the onset (Coggans: e-mail interview).

5.2.2 Statistical evidence

The main available statistical evidence[1] relating to computer security breaches are the Audit Commission's Survey of Computer Fraud and Abuse 1990 of 1500 organisations, and the National Computing Centre's Survey of Security Breaches 1991 of 883 organisations. The evidence from these survey's is supplemented in this study by a Quantitative Questionnaire of 200 respondents, full details of which are given in Appendix 1. The evidence from the two national organsiations makes the following main points:

1. Various forms of logical breaches were experienced in the following proportions according to the official surveys. Of the respondents in this study's quantitative questionnaire 83% have experienced one of the forms of logical breach. Unless this is widely unrepresentative, for some reason such as biased sampling, then the assumption must be that logical breaches are widely under-reported in official studies.

---

[1] The Audit Commission's Survey of Computer Fraud and Abuse 1990, National Computing Centre's Survey of Security Breaches 1991, Quantitative Questionnaire (c.f. Appendix 1)

Nature of logical Breach	% of total incidents
Disruptive software	35%
Unchecked software	14%
Unauthorised access via corporate terminals	11%
Staff misuse of resources	11%
Computer operator error	10%
Hacking	8%
User error	5%
Fraudulent input data	5%
Diversion of output data	1%
	100%

(NCC 1991:56)

Logical breaches by industry sector	% of sector suffering Breach
Distribution	43%
Transport and utilities	41%
others	36%
IT	34%
Finance and business services	32%
Local government	29%
Manufacturing	28%

(NCC 1991:39)

Breaches by Industry Sector	% of Sector suffering breach
Academic	5%
Commercial	14%
Public Service	11.5%
Other	0%

(Derived from Table 1 Audit Commission 1990: 9)

2.

> *Reported incidents of unauthorised access to systems via corporate terminals (i.e. by staff or contractors) were much more prevalent than external hacking* (NCC 1991:12).

The following data adds weight to charges that the legislative response to hacking has been diproportionate to the actual threat it poses. The statistics show that the majority of security breaches are carried out by personnel inside organisations rather than external hackers.

Malicious action by outsiders - 14%
Damage attributable to staff or ex-staff - 61%
(NCC 1991:57).

Audit Commission figures for the identity of the perpertrators of18 reported hacking incidents
9 - members of staff
9- undiscovered
(Audit Commission 1990:27).

3. The costs incurred due to hacking also tend to be significantly lower than incidents of insider-based breaches[2], computer viruses, and traditional forms of fraud that make use of a computer. This is both as a percentage of overall incidents reported and as a percentage of each category reported. That viruses are also more likely to be introduced by insiders (either accidentally or deliberately) exacerbates this fact.

Degrees of cost associated with categories of security breach as a % of total incidents reported for all categories

Costs of checking	Hackers	Insiders	Viruses	
Not significant	8%	68%	24%	100%
Minor	8%	56%	36%	100%
Major	7%	45%	48%	100%

(Data compiled from NCC tables 5.6: B.94)

[2] Defined as: access via corporate terminals, deliberate misuse by staff, fraudulent input data (e.g. invoices), Diversion of output data, Introduction of incorrect software, central operator error, user error.

Degrees of cost expressed as a % of each individual category's total number of incidents

Costs of Checking	Hackers	Insiders	Viruses
Not significant	33%	28.5%	20%
Minor	47.9%	55.6%	51%
Major	19.1%	15.9%	29%
	100%	100%	100%

(Data compiled from NCC table 5.6: B.95).

Audit Commission's figures of reported costs incurred from computer incidents for 1990

Fraud - £1,102,642
Hacking - £31,500
Viruses - £5,000

Impact of logical breaches	Hacking	Viruses	Inside Action	
Serious impact	25%	17%	58%	100%
Significant losses	13%	42%	45%	100%
Easily absorbed	7%	34%	59%	100%
Minimal impact	5%	36%	59%	100%

5.2.3 Quantitative questionaire data

The evidence from the qualitative fieldwork seemed to emphasise the perceived widespread weaknesses of computer systems. This study's quantitative data are explored in detail in Appendix 1, from which the following main points can be distilled: Only 25% of people felt their systems to be inadequately secured (Question 5). This may be explained, however, by the tendency of programmers to underestimate the weaknesses of the systems in their own environment.

The fact that much computing work is carried out by people without formal qualifications was mentioned in the main body of this study. Of the respondents 41.5% (Question 6) had no formal qualifications. This can be seen as due to both a lack of adequate levels of education in the computing industry, but also illustrative of the value of computing knowledge derived from practical hands-on experience rather than formal training.

Only 17% of respondents (Question 7) had no experience of some kind of security breach, 64% of respondents thought that insiders within an organisation posed more of a risk to its security than outsiders, whilst only 7.5% thought the converse (Question 14). The number of respondents who thought viruses and system breaking could be potentially useful was high. 40.5% and 67% respectively (Questions 15 and 16). Of the respondents 73% thought that the number of security breaches would increase in the future, compared with only 7% who thought they would decrease (Question 17).

Figures 4a-c show how both academic and commerical organisations experience hacking to a similar extent (62 and 63% respectively), although the academic sector is almost twice as likely to experience viruses. In general there is quite a high level of security breaches, with 25% of the academic sector experiencing all types of breaches and the commercial sector 18%. The data for those

experiencing no breaches is correspondingly low: academic sector 10%; commercial sector 25%.

The data also show that both the academic and commercial sectors did not view hacking or viruses as particularly serious threats (6% and 7% respectively in figures 4d and 4e). Hacks and viruses are perceived as constituting a similar level of threat, 9% of hacks/browses being thought to be serious and 7% of viruses (figures 4f and 4g). There are relatively high and comparable figures for the number of repeated breaches of both hacks/browses and viruses. 17.5% of hacks and 16.5% of viruses had been experienced more than 10 times (figures 4h and 4i). Finally, as a reflection of the perception that breaches are not a serious threat figures 4f-k show how 66% of both academic and commercial sectors think that their security is adequate.

5.3 REASONS FOR SECURITY WEAKNESSSES

5.3.1 The software crisis

Within computing, worries about security weaknesses can be seen as part of wider concerns regarding the nature of software production. These concerns are encapsulated in the phrase 'the software crisis'. There are various elements to the software crisis including the threats posed by computer viruses and the problems caused by the proliferation of different standards, shortages of skilled programmers etc. Peláez argues that, despite varying interpretations of what actually constitutes the software crisis, it is the: "gap between expectations and demands placed on software, on the one hand, and actual achievements of software, on the other" (Peláez 1988:178). There are two different explanations for this gap. One explanation emphasises the problem of the relative immaturity of the software industry: "We build systems like the Wright brothers build airplanes - build the whole thing, push it off the cliff, let it crash; and start all over again" (Peláez 1988:179). The second explanation of the gap between ambitions and achievements relates to the pressures imposed by the commercial environment: "users' illusions were actively promoted by the computer industry itself, especially by its marketing people ... Software was being produced in an environment of unreality, a fetishised even fraudulent environment ... " (Peláez 1988: 181).

The software crisis gave rise to a debate over how software should be produced and tested. The debate has been characterised as the 'science' versus 'craft' view of software development. The former emphasises how the production of software should emphasise the use of formal design methods to prove that the program will do exactly what it says it will, and so avoid the gap between expectations and performance. The craft approach prefers to emphasise the ways in which programs need to be responsive not only to mathematical proofs but also to the requirements of implementation in the real world.

Computing, in an attempt to overcome the software crisis, has increasingly evolved from the craft-like approach to the more scientific reliance upon standardised procedures. The knowledge involved has become increasingly codified, and the process of software production has increasingly concentrated upon what software should do and the internal consistency of those specifications. This has two main implications for hacking. First, the movement away from a craft approach has meant that those programmers of a creative but ill-disciplined bent have been increasingly marginalised. Wiezenbaum, for example, related how there were many examples of programmers at MIT who could produce concise and elegant solutions to programming puzzles (Brighton interview). Problems were encountered, however, due to the fact that the programs were produced by original, inventive, but sometimes idiosyncratic methods. In a commercial environment the utility of such programs could be severely diminished because of their lack of explanatory documentation. Upon the departure of the author, the remaining programmers would not be able to maintain or adapt the programs due to the fact they were not privy to the private logic of the initial author.

The second implication is that despite computing's increasingly more formal programming environment, the limitations of the engineering approach mean that hacking knowledge is still of potential relevance to security. Whilst the science-based approach enables verification as to whether a program will meet its specifications, the craft approach points out that there is no way of formally proving that they are correct. In other words, it prefers to emphasise the 'messiness of the real world' which mathematics alone cannot tame. Hence, the security of systems cannot be proved in advance because their implementation takes place in a changing environment. It is possible to assert, for example, that a system is invulnerable to certain types of attack but it is impossible to anticipate all the potential threats a system might face, particularly when human interaction with systems is involved. This inherent

inability to guarantee total security is illustrated by the various security weaknesses of which hackers make use.

5.3.2 The software crisis and the origins of hacking

Chapter 1 mentioned how the word 'hack' evolved from originally referring to a quick bit of work that achieves its aim, but is not done particularly well. The word became associated specifically with clever programming techniques. The meaning of the word evolved as it became more and more associated with the ingenuity of programmers forced to modify programs on an ad hoc basis until they met the often vaguely expressed requirements of the customer. This led to the originally perjorative dictionary definition of the word, assuming a more positive connotation as programmers' methodologically unstructured, 'trial and error' hacks achieved desirable practical results. Thus the origins of the activity of hacking itself stem from this craft-like quality of programming. This explains the origins of the first generation of hackers and hacking's lasting appeal to subsequent generations:

> For the craftsperson, results are achieved through clever tricks, and professional excitement is derived from 'not quite understanding what he is doing. In this streamline age, one of our most undernourished psychological needs is the craving for Black Magic and apparently the automatic computer can satisfy this need for the professional software engineer, who is secretly enthralled by the gigantic risks he takes in his daring irresponsibility (Peláez 1988: pp 201-202).

The image of programming, and by extension hacking, having elements akin to Black Magic is thus encouraged by the seemingly intrinsic baroque complexity of computing in the face of which anyone exhibiting practical knowledge receives the awe of the 'uninitiated':

> For thousands of years, man has been captivated by magic. People, gathered around campfires, would be spellbound by sorcerers. Using a wand and some exotic artefacts they would produce startling effects and the innocent would gaze on in amazement ... many of the sorcerers' techniques have been acquired by the mechanically adept ... Computer communication is still a black art, even to those in the computer world. For those in the know, this can be exploited ... The communications expert is, in his or her own way, a magician, able to conjure up vast reserves of memory and computing power at the touch of a button (Gold 1990: pp 47-48).

The Black Magic quality of hacking is also encouraged by its image of being a mysterious night-time activity and hackers' conceptualisation of themselves. An example of both of these points, is provided by a hacker who calls himself, the 'Dark Adept':

> A wizard is a person who believes everything is interrelated and attempts to find the interrelation and controls his universe by it. One such branch of wizardry is the Computer Underground ... I chose the handle The Dark Adept because I believe that out of darkness comes light. Out of the darkness of lies and oppression comes the light of truth and freedom. One just needs to be Adept enough to catalyse the reaction (The Dark Adept, CuD 2.15).

5.3.3 The problem of anticipation and the role of testing

(i) Intrinsic insecurity and serendipity

The frontier-like status of computing resulting from its relative immaturity is described below:

> The computer underground of today is the group that would have been the HAM RADIO operators of yesteryear. These radio operators could have made public radio impossible to hear if enough "EVIL" HAM radio operators would have decided to do this. In the long term commercial radio won out,

because everyone benefitted by the law and order that developed. The computer underground is just the group of people that always test the limits of the developing advances. They are the Lewis and Clark or Buzz Aldrin of this new territory. How we draw the maps, rules and laws of the future will depend on how and what they find (Forbush: e-mail interview).

The difficulty of anticipating a priori threats to security helps hackers expose security weaknesses by 'testing the limits of the developing advances'. A general quality of technological change is that the impact of advances may be double-edged. New car-brake technology, for example, may defeat the original objective for increased safety by providing a rationale for increasing cars' power and speed. Similarly, in computer security, new technical advances do not guarantee improved security. An example of this phenomenon is the use of fibre-optics in the transmission of electronic data. Fibre-optics were seen as reducing the potential for the tapping of data or 'electronic eavesdropping', however, hacking methods have already succeeded in compromising its security[3]. Counter cultural groups are often associated with the cutting edge of technological developments, for example, Sterling (1993) describes how the new communications technologies were largely pioneered by criminals, so much so, that: "In the early years of pagers and bleepers, dope dealers were so enthralled by this technology that owning a bleeper was practically prima facie evidence of cocaine dealing" (Sterling 1993: 183).

That security weaknesses in systems are seemingly inevitable is reflected in the experience of hackers' serendipitous opportunism. Schifreen, for example, was known as the 'Prestel hacker', for hacking along with his associate Steve Gold into the Duke of Edinburgh's private electronic-mail box:

I was playing with some software one day and found out that if you typed ten 2's for an id number on Prestel it was a valid

[3] c.f. Sterling 1993 p208

account. *Just by pure chance* (emphasis mine), I was just testing some terminals, I wasn't actually trying to get in. I hit the 2 button, ten times and it said 'yeah, fine what's the password?', so I thought 'this is easy, I know passwords are four characters so I'll try 1234', tried 1234 and it let me in and it turned out to be an internal BT account that let me access loads of closed areas on the system (Schifreen: London interview).

Schifreen's description of 'just happening' to find something out about a technology is related as a result of 'playing around' with it. What he perceives as attributable to chance, however, is largely based upon such basic security failings as inadequate user identification log-in procedure. Once he had gained initial access, subsequent entry to privileged accounts became possible because security was not maintained throughout the system. Information that allowed further progress was left lying around on the assumption that no one could have gained access because of the initial security measures.

Making a system relatively secure requires security measures at different levels of a system, thus taking into account that some of the first level security measures may be broken. However, even if systems are designed assuming that at any one stage previous security barriers may have been broken, total and 'pre-emptive' security for some artefacts may still be effectively impossible; as we have seen from the above discussion of the software crisis, it is in the nature of security that weaknesses cannot always be foreseen. They may only come to light as a result of the imaginative manipulations of hackers. The heterogenous curiosity of hackers allied with their 'instinct' for security flaws results in them eventually finding security loopholes in all kinds of technological artefacts. Thus Dell relates how he always keeps his eyes open for a hacking opportunity:

If I work or am on holiday I also see things where I think, "hey yeah, that's possible, last year I was in Miami and I found a

> way to park for absolutely free ... just by chance I found that if you put a dime in and turn the parking meter all the way up, as far as possible, and let it go all at once, because of the speed the meter goes, for one dime you can park the whole day. You develop an intuition, an instinct (Utrecht interview).

It is this instinct which is conducive to serendipitous discovery that security measures may always be struggling to contain, since the initial security breakthrough may not be due to the type of logical strategy that can be most easily anticipated within security measures.

(ii) The state of computer security knowledge and education.

Indicative of the security weaknesses of systems is the perceived lack of knowledge in the field of computer security:

> Contemporary insecurity and unsafety are basically built into today's IT architectures, but only very few people understand this (there is *no theory of secure and safe systems*!). Some hackers deliberately intend to demonstrate the apparent insecurity of contemporary systems (e.g. CCC), while others produce negative impact during unconscientious experimenting with parts of the technology (e.g. Morris' INTERNET worm) ... we have serious problems to understand what security and safety means, and we have *no theory of safe and secure systems*. In general terms, this has also been true for industrial systems where such measures had to be developed later (and the consequence of missing security and safety even being felt today, see: pollution). (Prof Brunnstein: e-mail interview).

Computer security ignorance is compounded by the tendency of those within computing to regard its effects as being overwhelmingly positive. This seems to be reflected in the way in which the technology is approached by software engineers:

> The general taboo behind contemporary IT is that everybody regards these systems as *positive*; only few users and even fewer experts realize that there is a positive side of the coin ('useful': Chip Chip Hurra!) connected with a negative one (bugs, viruses ...). Following the implemented moral categories, engineers regard technology as 'morally neutral', and they do not feel responsible for faults or misuse as they regard these as tasks of the users; unfortunately, users cannot understand today's very complex systems (mega bits of data/programs/data flow ...) to control the adequacy of IT results! (Prof Brunnstein: e-mail).

A general lack of education in the knowledge that does exist contributes to the continued existence of security weaknesses that could otherwise be repaired. Comparing it to a 'leaky sieve' Dr Cohen argues:

> The leaky sieve comes from the fact that OS designers don't know about protection, and treat it as an afterthought. Like most after-thoughts, the retrofit doesn't really fit. Why don't they know? Because they aren't taught about it in school. Universities rarely teach anything about protection. The average computer science graduate has only 15 mins on protection - that in an OS course where they are taught how to keep processes separate in memory. On the other hand, about 4% of the GNP is lost each year in most industrialized nations due to computer integrity problems. (According to some Lloyd's underwriter and several confirming research studies). Ignorance is not bliss - it is suicide (Dr Cohen: e-mail interview).

Cohen describes the effects poor education on the quality of security in industry:

> Crackers do not provide a service by breaking in - we know the situation is bad, and we know why - it is because computer professionals are ignorant and the fault should lie squarely with our educational system ... Computer security issues are ignored - or worse misstated by our teachers, and as a result, we have many people going in random directions making 20

year old mistakes ... Most crackers are simply using trivial holes left by ignorant programmers. I think any computer professional should be taught the limitations of computer systems and be given assignments to demonstrate these flaws in school. The situation now is like teaching how to fly airplanes but not teaching pilots that engines sometimes fail. Your system depends on your knowledge for its proper operation, just as an airplane does. We don't accept pilots that can't handle minor mechanical failures, why do we accept computer professionals that can't handle minor protection problems? (Dr Cohen: e-mail interview).

The consensus amongst hackers also emphasies the poor state of the conventional eductation system. They frequently describe their reliance upon self-taught or peer group-derived knowledge of computing and its security features. Schifreen, for example, describes the self-taught nature of his own computer knowledge:

> I didn't go to university, I did computing at school until o-level and that was basically the only computing education I got, the rest of it was self-taught for enthusiasm ... the knowledge you need for a computing job, doesn't correspond to the course work you've done at University or College. They're not teaching the things that are right for jobs (Schifreen: London interview).

(iii) Calls for hands-on experience

The perceived failure of the education system and the CSI to fully address security and operational weaknesses has led to calls for more practical 'hands-on' security knowledge. It is claimed that hacking may provide practical experience and a de facto education in computing and its security measures[4]. Herschberg, for example, defends hacking's status as an intellectual exercise that contributes to both theoretical and practical knowledge:

---

[4] c.f. Vinten 1990 p8

> Well, before I became a professor I was given many opportunities to do it myself, but that was in the very early days. The last time I attacked one with my own lilly-white hands must have been about 13 years ago, so I'm certainly to be counted amongst the first generation of hackers, as to being sympathetic, yes, I do accept, a technically satisfactory piece of hacking in lieu of the formal oral exam, providing it's well documented, providing it's not a trivial system and provided no harm has been done ... the proof of the pudding is in the hacking (Herschberg: Delft interview).

Herschberg is an example of those who believe that hackers' expertise at breaking into systems could be utilised in order to improve security knowledge. He and his students have been invited by various Dutch companies to attempt to access their systems and to give a full report of any security weaknesses found. His seemingly idiosyncratic views on the benefits of hacking are fuelled by the contention that computing is in great need of a combination of both academic theory and 'hands-on' direct experience of computer security. He describes how he has:

> a continuous trickle, it's not more than one or two firms at a time, who want me to investigate the only way there is, which is penetration. As an academic, I have one continuous complaint about security: there is no theory; almost no theory. There is some theory, there is cryptography which is quite respectable academically and therefore has a great deal of worthwhile interesting theory, there are a few other areas, say inference from systems one may interrogate interactively. Again, the problem lies, as Dorothy Denning has pointed out, that, by putting the right questions the user may reach information or may infer information he was not meant to possess. That at least has the beginnings of a theory behind it. For the rest, let's say the general penetration attempt is hardly covered by the theory, so that the only way to find out about it is to take the experimental approach: wade in, do it (Herschberg: Delft interview).

Thus, Prof Herschberg argues that the theory will only come through the lessons gleaned from practice: 'wading in', and like Rop, he sees computing and the hacking of systems as still very much a frontier activity, the best comparison to be made:

> would be with the early days of say radio. Marconi successfully transmitted accross the Atlantic before there was a theory of terrestrial radio-wave propagation. The Wright brothers flew by the seat of their pants, theory came much later. I think it's fair comment that any new technology must go through the stage in which theory lags far behind practice. It is true for security except for shreds and patches, so I see no other way than actually to attack a system in order to make a valid statement about it's penetrability (Herschberg: Delft interview).

The actions of hackers, whether deliberate or not, serve to illustrate security weaknesses in an area where theoretical knowledge tends to be subsumed under the exigencies of practical applications and interactions of programs and computer systems:

> As the importance of IT will grow further, we will need better understanding of risks inherent in IT (e.g. concepts of inherently safe and secure systems), as well as risks from its use and misuse. Only IT-inherent risks may be analysed independently of its application; the terms 'safe' and 'secure' (which are semantic categories, rather than syntactic ones!), may only be defined in terms of an application, and therefore a theory of safe and secure applications may only be defined after hands-on experiments (Prof Brunnstein: e-mail interview).

Herschberg's view that security knowledge could be improved by analysing the techniques of hackers, draws attention to the issue of the correct degree of responsibility and blame to attach not just to the perpetrators of security breaches, but also their victims. The ethical issue for Herschberg centres more upon the moral requirement facing those in charge of systems to maintain security,

than to blame those that breach security. Hackers are criticised because without their existence, there would be much less need for security in the first place, and therefore on balance they amount to a waste of resources. Herschberg's rejoinder to this emphasises the practical safety issues hackers give rise to, rather than the waste of resources that may be attributed to them. A successful hack, defined as gaining super-user status in a system, means that the hacker may obtain complete control of a financial or a safety-critical system:

> The fact is that you can't by their actions, at least not easily and not from the outside, tell a hacker from a criminal and you never know at what stage criminals do get interested. Quite apart from the fact, at least all major enterprises, and that includes the entire financial scene, have a vital concern to have no intruders, whatever their origin, or whatever their purposes ... that point that if there were no hackers there would be no need for security, does not follow since there always is a prima facie suspicion of somebody being out to, let's say, distort the uses you put your system to; you better employ a hacker because your criminal might have designs on you. An ounce of prevention is better than a pound of cure (Herschberg: Delft interview).

5.3.4 The knowledge gap

An illustration of the perceived need for more hands-on experience is the alleged knowledge gap that exists between the CSI and CU. For the first time, a new generation of young people are growing up completely at home with computers and their capabilities. Herschberg claims that:

> What we are confronted with is a generation that has lived with computers virtually from the cradle, and therefore have no trace of fear, not even a trace of reverence. To me, a computer is still, well, something to be revered. When I started my career in computing, there was'nt really computing at that time ... there were about three of them, you had one shot at a run a day if you were lucky. It was sacrosant, it no

> longer is to those kids, you go in, have a bash at the keyboard, they're convinced by experience that nothing much can go wrong. (Herschberg: Delft interview).

One manifestation of the fundamental nature of the perceptual divide between hackers and the establishment is vividly described by John Perry Barlow in "Crime and Puzzlement". The hacking community, having grown up with computers almost 'from the cradle', stands in opposition to an establishment of law-enforcers largely ignorant of computing. Ignorance leads to mystification of the opponent, for example, in Barlow's dealings with hackers he described how, "I have since learned that while getting someone's TRW file is fairly trivial, changing it is not. But at that time, my assessment of the crackers' black skills was one of superstitious awe. They were digital brujos about to zombify my economic soul." (Barlow 1990: 47). Barlow proceeds to describe the implications of such fear and ignorance when it emanates from the establishment. He was interviewed by an FBI agent, Agent Baxter, in connection with the 'stealing' by a hacker of proprietary Apple Macintosh source code on behalf of a group opposing the commodification of software: the Nu Prometheus League. Agent Baxter's lack of knowledge was typified by his frequent references to the 'Nu Prosthesis League':

> Poor Agent Baxter didn't know a ROM chip from a Vise-grip when he arrived ... You know things have rather jumped the groove when potential suspects must explain to law enforcers the nature of their alleged perpetrations ... he took to ... saying 'My eight year old knows more about these things than I do.' He didn't say this with a father's pride so much as an immigrant's fear of a strange new land into which he will be forcibly moved and in which his own child is a native. He looked across my keyboard into Cyberspace and didn't like what he saw (Barlow 1990: pp 53-54).

Mischievous rebelliousness is typical of the hacking fraternity. It is consistently evident in the way hackers' minds perceive unorthodox ways of manipulating any given technical situation. Due

to increased technical outlets for this inventiveness, the latest generations from which modern hackers draw their numbers have a qualitatively different experience of computing to those who tend to be in charge of systems, and responsible for the creation and implementation of legislation designed to stop hackers.

Authors such as William Gibson are popular with hackers, along with films such as "Brazil". Two aspects of both these works that the hackers find affinity with are the way they represent individual opposition to a monolithic technological order and their portrayal of the contrast between life "on the street" and life sheltered by the priveleges of power and/or money. This concept of "street life" has been internalised by parts of the computing community. Urban teenagers base their experiences and subsequent feelings of isolation from authority on the fact their lives involve a level of "street-cred" ignored by, and foreign to, the establishment. Hackers, too, due to their lifestyles and single-minded approach to their activity, distance themselves from "the suits" or "neck-ties" (two phrases frequently encountered in interviews with hackers).

To the extent that computer security is lacking in a theoretical grounding, the only true way to test security is to actually attempt to breach a system. This requirement for practical knowledge has put pressure upon some of the conventional "experts" in the field of computer security. In this area, theoretical knowledge tends to be gained at the expense of detailed specific knowledge. Often a "security expert" with a good grasp of the general tendencies of most computer systems is at a disadvantage when it comes to the question of the exact details of a specific system. A hacker will research his narrowly defined area of specialism in an exhaustive and comprehensive manner, in an amount of time and to a degree not feasible for a computer security consultant. Onderwater from the Dutch Criminal Research Institute recognised this and pointed out that it was impossible to know everything about every system, and in his job, he relied heavily upon networks of specialists to obtain the exact information he needed. This specialism is the quality most prized in the hacker community and inevitably not obtainable for

computer security professionals working within the confines of a conventional job-structure. Similarly, Kevin Mitnick, the 'dark-side' hacker, when asked whether hackers tended to have an edge in their 'skirmishes' with the CSI, described how:

> They've got the motivation and don't forget, computer security people go to their job from nine to five, for hackers it's a hobby. You dedicate more time to that hobby than you would a job, when you're done with your job, you want to get out of there, go home to your wife, play golf, go work out at the gym. You don't want to sit there and deal with it, usually. But hackers, on the other hand, devote hours and hours to learning, so a lot of them are more talented in maybe that narrow area of computers (Mitnick Amsterdam-USA phone interview).

This type of knowledge gap between the specific knowledge of the hacker and the general knowledge possessed by the computer professional is reflected in their different interpretations of particular incidents and the lack of shared values between the professional security experts and the hacker. Gene Spafford has been described as one example of a well-known and influential figure on the net who amongst the hackers I spoke to, is a figure of derision, a man they view as largely out of touch with the reality they experience: "Yeah, well, he's an ass-hole" (Mitnick: Amsterdam interview).

Schifreen describes the knowledge-gap with respect to his ambivalent relationship to the CU and CSI:

> I'm bridging the gap because that's the way it's got to be done. Yes, you've got the security consultants like a big city accounting firm that will come and talk to you, and they know the theory because they've read the books and talked to the manufacturers and certainly they can give you some good advice. But they're not involved in the real world, they sit at their desks writing articles, books and reports, they don't talk to hackers, they have'nt been on the end that I have. They don't keep their ears to the ground, they don't know what's going on, they know what's going on by reading product

reviews and certainly there there are management principles that you can go around telling people and they are always relevant, but unless you've got the mind of a hacker and you think as a hacker thinks, you won't realise where the loop-holes are in people's security systems (Schifreen: London interview).

This shows how the 'knowledge gap' is rooted in the difference between theoretical concepts and guidelines to security and the 'nitty gritty' of real world computing situations where security weaknesses exist in the rich texture of incrementally growing and adapting computer systems.

5.3.5 Commercial pressures and security holes

One of the underlying reasons for the level of ignorance described in previous sections is the perennial problem of scarce resources. Spafford, for example, complains that education in security issues has suffered as a result:

> We're producing students that don't know enough about software engineering, about safety of software systems ... I have to teach them on equipment that is very often several years out of date, that is underpowered, that is lacking in basic tools that they will be using when they go out into industry ... there are institutions that are producing students whose sole education is done either on PC's using MS-DOS or some kind of batch-operating system, I know of places that are still using punch cards (Spafford: e-mail interview).

Thus commerical factors contribute to the continued existence of security holes:

> It's because the bottom line in any company today is making profit, you've got no time to do anything that doesn't bring you money or makes you profit. British industry in general is in a hell of a mess and in particular all the staff who could be squeezed out of work in any enterprise, have been squeezed

> out. There's no time for non-productive work which is the security issue ... everything in the computing industry like everywhere else is done in a hell of a hurry to get it done yesterday. A lot of rather poor programs get written (Dr Frank Taylor: Knutsford interview).

Specifically, the following six factors create conditions conducive to the continued existence of security holes.

(i) Commerical pressures - job structure

Commercial pressures are evident with respect to the way in which computer security jobs are structured. Detective Harry Onderwater of the Dutch Criminal Research Institute's Computer Crime Squad, complained that computerisation has taken place within companies with scant attention being paid to adequately educating those given jobs involving close contact with computers. He described the informal and ad hoc way in which he found himself involved in the issue of computer security:

> I got system manager next to my job at the Drugs Squad, because there was no system manager and I was the only one who could work with computers, so I did the computing ... I think if there had been somebody specialised then, they could have done the job better than I. It's hobbyism of the guys who work there, it's a problem also with the money involved...they won't make a system manager but leave you at your old job and do that next to it. Courses are very expensive...it's a job you do next to your own job, a lot of functions should be divided over more people, maybe a system manager should never be the same man as a data-base administrator, but because it's a small firm, the guy is a system manager, a data-base administrator, a security officer and he's also the book-keeper (Onderwater: Hague interview).

Schifreen also draws attention to the ad hoc way that jobs are structured for security personnel, arguing that it helps contribute to the generally security-ignorant nature of computing in industry:

> apart from most people not knowing what they're doing ... another problem is that, let's say you've got a large company and they suddenly read a book and it says 'make sure you've got a security manager'. And they think, 'right, who's next in line in promotion to manager? So and so down the corridor. Get him in, congratulations, you're now a manager. 'What of?' 'Security: go and read this book.' The average security manager according to recent research, as they say, has been in the job for 8 months, so there's no way that they've got the experience to know what the risks are, and reading a theoretical book is not going to tell you where the risks are (Schifreen: London interview).

Thus there is a prevalence of underqualified personnel attempting to deal with security problems. In addition there are the poor administration practices that exist in many organisations:

> I am forced to agree that most computer managers are just about as incompetent as most crackers; they merely apply 'formula' solutions to problems with no real understanding of what they are doing. To the extent that crackers are exposing this lack, perhaps they are doing a service to the industry and perhaps we will eventually see truly professional computer managers and security staff hired by companies, rather than the 'clerks' that they use now (Bickford: e-mail interview).

The reason why those in charge of security are often particulary unsuited to the job is the result of the low esteem in which security work is often held.

(ii) Low profile of security

Computer security in the commercial sector adopts an inevitably low-profile because any successes are negatively defined. If a conscientious security officer presides over a trouble-free system, then it:

> unfortunately creates the impression, a very negative impression, of no actual achievement to point to. The proof of the achievement, if any, is in the absence of penetrations or penetrations come to light, which is a different thing ... virtually everybody's successes are more visible than those of the security officers. Therefore, it is good for your career development, not to be the security officer or whatever title he may bear in the organisation (Herschberg: Delft interview).

(iii) The constant need to update

It is also common that even when technical fixes have been made to fix security flaws, the latest update of the system incorporating the fix is not utilised by an organisation. If organisations use the very latest operating system from a vendor it tends to be relatively secure. However, to avoid the expense of constantly updating, earlier versions of operating systems tend to be used and left untouched and may not have been upgraded for a number of years:

> The best example of this is SunOS 3.5. There are many, many holes in that system. And there are many, many sites that still run it, because the upgrade to SunOS 4.0 just wouldn't run on many systems without expensive upgrades. Even on newer systems, finding the resources to do something as simple as pulling over a patched version of a vendor's utility can be difficult to get done (Holbrook: e-mail interview).

The ever-present commercial pressure of limited resources leads to ad hoc alterations of systems in order to increase their perfomance, but this may lead to an intrinsic mismatch between a system's nominal security and its actual secureness, taking into account the way the system actually functions on a day to day basis. In addition, few if any systems have been designed from the bottom up with security as a primary objective. The quality that sell computers (as with cars) is raw power rather than security features. The following quotation highlights how such pressures interact:

> Yes, Von Neuman architecture is *inherently insecure*, as concepts of 'security' and 'safety' have not been fully realised (or even reflected) in its basic concepts. Example: while a secure system would deny illegal services *in its innermost kernel*, contemporary security is implemented *on top of today's system*; if you succeed to penetrate the shell, the kernel is open for any action. As the current trend optimizes performance (more storage, faster processing, broader and faster channels and devices), concepts of safe systems are forgotten even where some hardware features (such as: protection bits) are available (Brunnstein: e-mail interview).

Rob Nauta, a Dutch hacker, illustrates how agreement over failure to fix holes spans both the CU and the CSI. He gives the following example of the ways in which the activity of hacking may be beneficial to the computing industry, by drawing attention to program holes, even if it is not particularly original:

> The OS is being sold by a company, not the programmers. Hence the company weighs profit and minimising costs (avoid updates) against loss of sales due to bad publicity (the general image of the OS as good, or bug-ridden). Thus patches and updates are only released when necessary. A company like SUN listens much to the customers, which are academic sites and research companies. Most bugs are found for SUN's since they are the most used computers, but all get fixed soon. Companies that sell to business managers deal with the management who don't follow the news and are more influenced by advertisements than by word of mouth. Hence HP-UX (HP-SUX is its nickname), IBM's AIX and DEC's ULTRIX are notorious for the time it takes to fix anything (Rob Nauta: e-mail interview).

(iv) <u>The problems of updating: the responsibility of the vendor</u>

Closely allied with the expense of updating is the time-consuming technical problem of upgrading future releases of a system. Moreover, it is seen as neither commerically desirable nor

financially possible for sites to maintain the expertise needed to constantly identify and fix bugs, as their main job is seen as providing the users of a system with various facilities. The real job of maintaining bug-free systems is, SMB contends, that of the system vendors:

> Most individual sites are not in a position to fix bugs. Even if you have source, you generally don't want to make any more changes to the distributed system than are absolutely necessary. I'm speaking here from my vantage point as a former systems' programmer -- the more you diddle, the harder it is to upgrade the next release ... The real responsibility is with the vendors. They need to provide more secure systems. It's hard, because security is always a tradeoff with convenience. But they have to stop taking shortcuts in their system architectures (Smb: e-mail interview).

(v) The exaggerated claims of marketing

The potential for security breaches is exacerbated by the exaggerated claims of marketing. They lead to a lack of coordination/symmetry between what a system is promised to do and what it can actually be made to do: "Marketing, of course, and the way business is run in general, have a lot to answer for. Promise anything, *then* figure out how to (or if you can) deliver. Make the sale. If that involves telling people that all they have to learn to perform an incredibly complex task is to push one button, then tell them that." (Rob Slade: e-mail interview)[5] Marketing puts pressure upon technical staff to produce improved systems. These systems may work, but the hurried nature of their construction means that adequate security features are often lacking. Dr Cohen describes these marketing pressures which guarantee the continued existence of the 'leaky sieve':

---

[5] c.f Pelaez's (1988) description of the marketing of IBM's 360 family of computers.

> So many holes because so few 'experts' know about them. So many holes because making things work right takes more skill than making them barely work at all, which is what the research people do- get things prototyped. Unfortunately, prototypes go into production so fast that we cannot get them fully sorted out, so we leave big holes so we can fix operational features - leaving enormous protection holes in their place ... there are surely many reasons - but I think the most important is a marketing reason - people won't pay to make themselves safe - they would rather buy the newest upgrade of the wordprocessor. They can buy insurance from an insurance company (Dr Cohen: e-mail interview).

(vi) Apathy and hype

There was, in the view of a broad cross section of interviewees from both the CU and the CSI, a general feeling that approaches to computer security were also often apathetic. Tozer used the example of motorway accidents: on the stretch of motorway following the scene of a recent crash drivers only temporarily slow down in reponse to the safety concern caused by the sight of the crash. Similarly, after a computer security breach has received large coverage in the media, organisations tend to be more concerned about their security, a concern which quickly fades once the short term memory of the breach has faded. The result tends to be alternating periods of apathy and over-reaction with regard to computer security services. Even when attention is focused upon such holes it may often fail to address the underlying security weakness, due to the exaggerated and misdirected nature of the response.

Efficient security work seems destined to pass unrecognised and unrewarded in any commercial career structure. The converse of such low profile security work is the 'hype' that surrounds those that have made a deliberate decision to make security their business:

> Let's try and distinguish between people who look after security in the usual organisation and people in the security

> service industry selling computer services. The people in fact in the user industry have got to keep a low profile and have their job done well when no-one hears about them. When someone hears about them and a breach has been made, then they get a high profile which is destructive to their job. The essence of their success is having a low profile because they've protected the systems they're responsible for. In contrast, the service industry is concerned with publicising, hyping up any breaches of security that have occurred, so that they can sell their various protection devices; anti-virus guns and the like (Taylor: Knutsford interview).

The computer security industry has thus been accused of promoting fear about security breaches in the form of hacking and viruses in order to increase its business. The exaggeration of the risks of security breaches can, for example, take the form of using dubious figures for the incidence of computer crime. A more specific example of the deliberate manipulation of information concerning computer security is the instance reported by Dr Cohen. An article he had written on the subject of the possibility of the development of benevolent viruses was altered by the publishers:

> they mangled it to promote the protection business. The main point of the article ... was that benevolent viruses are possible and that only the computer security industry wants to claim that they are not - and the reason is so that they can scare you into paying them ... there is a tremendous risk in an uncontrolled protection racket that goes by the name of 'computer security'. If I told you your house would burn down unless you paid me $100/year, you would probably report me to the police (and wonder why I charged so little). If someone in the protection racket tells you your computer will crash and you will lose all your data unless you pay them $100/year, how is that any different? (Dr Cohen, RISKS 13:53).

The prevalence of ignorance regarding security measures can give rise to an exaggerated response to the issue of security. It can also, however, give rise to apathy. This ambivalence was apparent in

the quantitative questionnaire response to question 17: 23% of respondents thought the computing industry's response to hacking was excessive or hysterical whilst 26% thought that it was insufficient.

Tozer, as an educator in security issues, expressed his constant frustration concerning the lack of care organisations take over their security, and consistent with the examples given previously, he underlines the manner in which the way jobs are structured affects how the provision of security is approached:

> I still blame a lack of professionalism amongst Data Protection (DP) managers, for allowing things to occur. It's their job ... but you get very few DP people at the board level anyway, even though DP penetrates everywhere. So even if they do know what they're doing they don't even get a chance to put it at the same strength as the others ... For years I've been trying to find out what's needed to trigger peoples' minds in the right channel. Last week for example, I got a phone call from a very well known company. Could I give a course, a data-protection course?..he said these are people at the top, so I said it shouldn't be too difficult ... I'll send you a sheet and fill in a few questions and we'll see how long it'll take. "Oh, well, they've only got two hours!...I mean a day, yes, for senior people, but two hours? (Tozer: Hawarden interview).

Security weaknesses are often an integral part of the computer system as it networks with other systems. Nauta accuses the vendors of paying scant attention to security considerations in the design stage and responding apathetically to the need to rectify such faults when they are identified:

> Most bugs are found in networking code, since it runs at the system level, yet it is accessible by user programs. Most network protocols were designed without concern for security. NFS has no security at all, but SUN now allows to require (sic) a reserved port, which is a first step. NIS (YP) is also a good example. I wrote a program called YPX which could retrieve the password file from any machine, it has caused a SUN patch to be issued. Other vendors haven't announced anything,

people are already complaining, I wonder if the other companies will ever bother to fix it (Nauta: e-mail interview)

5.4 THE RATIONALE FOR HACKERS

(i) The potential for cooperation

Faced with the extent of security problems described, hackers sometimes make dramatic claims regarding the extent to which their activity improves standards of security within computing:

> Without hackers, computing would be a boring, drudgerous tool people would use because they need to get something done that they don't want to do. Hackers are computer enthusiasts more than anything else; it is through their enthusiasm for computers that they were able to find security bugs. If you consider a 'hacker' someone who unlawfully enters systems, then without hackers the nation would be nakedly awaiting serious attack from thieves and foreign agents. I have no doubt in my mind that the existence of hackers in this country has been a beneficial one except for certain well-documented cases; cases which would have been much worse if it had not been for hackers before them who have been able to close off the more wide-open security flaws/bugs (Maelstrom: e-mail interview).

This argument can then be further divided into the claims that hacking can be either a direct or an indirect benefit to computing. Direct benefits would stem from innovations in programming methods and security, along with hardware developments. An example of this would be Levy's first generation of hackers.

With regard to the indirect benefits of cracking, it can be claimed that the existence of hacking has led to a general climate of improved security consciousness and that this has led to 'trickle down', indirectly related improvements in data security. Thus, for example, potentially crucial data can be lost to a business due to the usually insured risks of fire, flood or theft, but it can also be lost due

to a system failure that coincides with poor back-up storage procedures for data. An indirect benefit of hacking, therefore, is that faced with the fear of external threats to the security of a system and its data from hackers, system operators are more liable to make regular back-ups than they might usually otherwise make. These regular back-ups can then provide insurance against accidental losses of data from events other than hacking incidents. The system becomes more secure than it would have been originally, due to awareness of the possibility of being hacked.

An additional argument in favour of greater cooperation with hackers is that greater access to systems tends to make 'hacker-types' more responsible computer users, who are then more liable to make productive use of the security knowledge they have gained illicitly. In the case of John Draper, this actually led to him 'punishing' users on the system he was in charge of, in the event that their hacking led to behaviour which adversely affected other users on the system. From his experience as a system manager, he claimed that:

> it is clear that by closely working with potential hackers and students, you can go a long ways in cutting down malicious hacking. I took a firm hand in keeping them in check, while at the same time, I tried to direct their energies into useful productive work. One thing I remembered was a HACKING CONTEST (under tight supervision) where I challenged them to break into the library account, and if they succeeded (and told me how they did it), they would get three months free usage ... Several people broke in, and I had about 2 people dedicated to helping me, and found a security flaw in the system. In this case, BOTH were winners. So yes!! There can be a positive lesson learned here, and that is to adopt a less fascist approach when dealing with hackers, and be less 'Punitive', but firm when dealing with them (Draper: e-mail interview).

Mofo also gave the following detailed account of his experiences of the potential that exists for cooperation between those in charge of security and those who enjoy testing it. His description

reinforces the previous discussion of the significance and desirability of direct 'hands-on' experience of security issues:

> I've gained knowledge on how to make computers and their operating systems more secure. Instead of complain about it and act foolishly (i.e. involving Keystone Kops), I took a proactive role to determine intent and repair the situation as best I could. My preference is to deal with intruders as human beings. In my experience, 'crackers' have been very receptive toward that attitude. Since my systems are always backed up on a regular basis, the few destructive 'cracking' attempts have been relative non-events. The admin community as a whole seems to be quite paranoid about security information and their highbrow attitude leaves experience as the only expert tutor (Mofo: e-mail interview).

A more damning indictment than the charge of being 'high brow' is made by Coggans, ex-Legion of Doom member, and now one of the founding members of ComSec Ltd., a computer security firm staffed by ex-hackers. His claim is that:

> The computer security industry is a farce, the key players who hold the majority of clients are the big 6 accounting firms, with Deloitte & Touche and Coopers and Lybrand in the lead. I wouldn't ask a mechanic to perform a triple-bypass on me just because he understands valves, no more than I would want an accountant auditing my computer security just because he does the financial audits of my accounting programs ... One company we contacted had an audit by one of the accounting firms. An auditor was onsite for 10 hours a day for 8 weeks. The report came back saying that they should put an exit sign in the computer room. This same company had a PBX controlled by computer, a dial-out option on the PBX active with the code 1234, and an AS-400 with poor password management. I noticed this upon initial contact. But the accounting firm had already turned them off to outside security audits, so their problems still exist. $100,000 for a damn exit sign (Coggans: e-mail interview).

This feeling that 'legitimate' computer security providers are out of touch with the practicalities of intrusion prevention is an important element of the rationale that hacking should be recognised as a valuable resource to improve computing standards[6].

(ii) The industry benefit argument

In Chapter One, we saw the various generations of hackers that have evolved since the earliest days of computing. Hacking, defined loosely as the inquisitive manipulation of computers, has historically played a major part in the development of both computer hardware and software. The energies of hackers helped to revolutionise computing from the cumbersome valve-dominated technology of its early days to the mass proliferation and dispersion of personal computers by such pioneering hackers as Steve Wozniak of Apple Computers. The contribution to positive technical developments from the latest generation of hackers, crackers, is perhaps less easy to identify due to their largely underground status. An example, of some of the practical benefits the computer industry can gain from the most contemporary form of hackers, however, is given by Jean-Bernard Condat of the French Computer Chaos Club who describes how:

> When a hacker works, three months after, the bug that he uses will be discovered and/or repaired. In France, it's 75% translation of bugs from American programs and 20% of normal password indiscretions. Some of my members are building a well-known program (available in three months) that help end-users or customers of great computers to find easy-to-understand password ... but-hard-to-find, too. The dictionary of such a program is terribly important and these 5 boys are using all the available time to build this extremely useful program[7] ... already sold to two big companies in Paris! (Condat: e-mail interview).

---

[6] It forms part of what has been previously referred to in Chapter 5 as 'The Knowledge Gap".

[7] The usefulness of such a program is tacitly conceeded by the experience of security personnel, one of whom, John Holbrook, from the Computer Emergency Response Team, is quoted in the next

Substantive criticisms are made of the ability of non-hacker, establishment-type firms to provide an adequate appraisal of the security status of a system:

> In theory, actual hacking would be the best way to 'debug' security procedures. In practice, only outsiders can look at a system from an unbiased viewpoint, so this opens up potential security problems. Part of what we do at ComSec we call system penetration testing. This is an audit of external security practices currently in effect by subjecting them to a hacking attack. I personally think this is THE ONLY WAY to get a snapshot of security problems to get a foundation of what needs to be fixed, but only an outsider can do it accurately. We go in with only a release form. No passwords, no dialups, no information at all. We return a report outlining all dialups, passwords, and information gained. This leads indirectly to an internal audit to fix the internal errors that left the systems vulnerable to outside attacks (Coggans: e-mail interview).

(iii) Potential underestimation of the role of hackers

It has been shown that security weaknesses can be due to incremental alterations of a system as a response to commercial pressures which can inhibit the full realisation of security improvements. Also, there is the problem that even if a system is technically relatively secure, it may be vulnerable to manipulations of its human element: that is, the 'social engineeering' of operators and employeess that interact with the system. Hackers, it can therefore be argued, are a means of drawing attention to either previously unknown security weaknesses, such as the poor interworking of programs or vulnerability to social engineering, or to known security problems that have not been addressed due to commercial pressures.

---

chapter as attributing 75% of the security breaches he encountered as due to poor password choice and maintenance.

One reason why this potential may have been underated is the fact that hackers do not generally publicise their findings of security weaknesses in conventional channels. Those that notice hacking information on their bulletin boards, however, may then report the faults the hackers have documented, a fix will then occur, but hackers will not receive recognition for the impact of their activity:

> In general: finding errors in installation (mostly bad file protections), as done by a tool like COPS, is useful, since beginning crackers (sic) use these. Bug fixes are hard to do yourself, and just a bug report won't get the bug fixed, enough people must complain about it. That's why publicity about bugs is a good thing. Whether to report them is another thing, I inspired 2 SUN bug fixes with my programs (cover.c, which used a fault in telnet, and ypx which uses YP design oversights), yet I don't get credited, but the people who saw my programs and sent them to SUN do. It's a strange world ..." (Nauta: e-mail interview).

Thus the belief that hackers are unoriginal and contribute little to security knowledge may, to some extent at least, result from a failure of such knowledge to be correctly attributed and accredited to a hacking source. A failure that may be exacerbated by a reluctance upon the part of hackers to freely publicise and disseminate their knowledge due to fears of prosecution and general hostility from the CSI and legal establishment.

5.5 RATIONAL FOR NON-COOPERATION - 'THE HAWKS'

There are two main strands of the CSI that stand in identifiable distinction from the computer underground, and whom therefore, do not contain some of the confusing inter-group qualities of the 'poacher-turned-game-keepers'. These two strands of the CSI could be characterised as the 'hawks' and the 'doves'. The basis for the different interpretations of the character of hacking rests upon two main aspects. Firstly, the hawks and doves dispute the ethical content of hacking activity, the subject of the next chapter. Secondly,

they dispute the extent to which hacking is technically relevant to computing, the extent to which cooperation with hackers could potentially produce technical benefits.

(i) Technical arguments against hacking

The ad hoc and largely unsolicited testing methods of hackers, do not fit well into the professional structure and requirements of the computing industry. The unorthodox aspects of hacking are not conducive to establishing a rapport between those obtaining knowledge about the security of systems, by illicit, unauthorised means, and those in charge of maintaining the systems who could benefit from such knowledge. This is due to two main reasons. Firstly, the nature of much hacking activity does not sit well with members of the computing industry who tend to inhabit a technological environment where discipline of method and obedience to instructions tend to be valued more than evidence of unstructured and generally un-documented technical brilliance. Secondly, the unsolicited nature of illicit hacking means that systems are being used without the prior permission of the owners. These two factors lead to a situation that gives rise to an immediate lack of affinity between hackers and the CSI.

The call for more emphasis upon the practicalities of security stands in opposition to those calling for a more formal approach to security. One criticism of the idea that hackers provide a useful research and development resource is the contention that hackers very seldom make use of any original security weaknesses. In addition there is the contention of Prof Spafford that:

> All that breaking into a system teaches is how to break into systems. It's very similar to testing software with random testing, for instance. If the procedure fails, what knowledge has been gained? Does it mean that the system is secure? Does it mean that the cracker didn't try hard enough? In testing, if a set of random test fails, we cannot conclude the software under test is correct (I can give you, scores of references on

this). It is only a crude approximation, and is viewed as 'real' testing only by the uninformed (Prof Spafford: e-mail interview).

Coggans (e-mail interview) points out that some computer systems are safety-critical to the point that human death may be a result of any system failure. In so far as this chapter has shown that hacking offers the potential to provide useful information with which to remedy some security weaknesses, the question remains as to why more use is not made of hackers' expertise. Fuller cooperation with hackers to use this expertise may be problematic as illustrated by the practice of 'security through obscurity' whereby the CSI avoid cooperation with hackers. This is because cooperating with hackers may provide security practioners with useful information with which to fix security holes, yet it also threatens to increase the knowledge of hackers by offering them more access to potential hacking targets and opportunities for social engineering[8]. Unsolicited hacking activity is also problematic because it threatens to damage the delicate nature of many modern inter-connected systems.

> Hacking can provide us (information security, audit, vendors, etc.) with information about vulnerabilities. Yet, the problem today is that the stakes are too high for this type of teaching to continue. Specifically, the interconnected world is too fragile to allow 'volunteers' to test the security of organizations without being invited to do that (Sherizen: e-mail interview).

This leads directly to the subject of whether cooperation should be encouraged between hackers and the CSI, or whether computing is for the forseeable future to be characterised by a confrontational situation of 'them and us'. The idea that there should be cooperation between hackers and the CSI is hotly contested by some members of

---

[8] Defined as tricking legitimate personnel into aiding illicit intrusions, for example, by deceiving a telephone operator into giving security information by pretending to be a telephone company engineer.

the CSI who argue that the educational benefits to be derived from hacking are exaggerated:

> I think it's a misconception to believe that most (emphasis: 'most') hackers have expertise that's particularly worthwhile. Many, of course, work from cookbooks, lists of known holes. While such lists are useful to the vendors and to CERT, they're in some sense, uninteresting -- few, if any, show any degree of conceptual novelty (Holbrook: e-mail interview).

Despite such a contention, diverse figures from the hacking community have used their hacking ability in the wider computing community. Thus Schifreen, Van Os, Coggans and Mofo, have all utilised their knowledge for commercial purposes by starting up computer security firms, whilst Prof Herschberg and his students have acted on a consultancy basis for a 'steady trickle' of corporations willing to have their security tested by 'hands-on' methods. In contrast to this experience, however, Prof Spafford puts forward the following argument:

> A true computer security specialist learns about more than just weaknesses - she/he should learn about issues in software engineering, formal methods, testing theory, operating systems, language design, human factors, risk assessment, the law, networking, cryptography, and a number of other topics. Breaking into a system teaches NONE of these things - it simply serves to illustrate how poorly configured many systems are, and how poorly tested the software is. But that should be obvious to anyone studying software engineering or security! (Prof Spafford: e-mail interview).

Cohen also emphasises the point that within computing there is a general awareness of widespread inadequacies and faults in many systems, and so hackers' actions provide little original security information:

> I've never seen a 'cracker' who broke into a system in a particularly novel way. Every attack of this sort is one we

have known about for 20 years and just not acted on. It's like taking candy from a baby. What we need is fewer computer security babies and more well-educated experts (Dr Cohen: e-mail interview).

This tendency for the majority of hackers to make use of unoriginal security weaknesses is recognised by some of the hackers themselves. Thus Nauta agrees that:

> Most crackers are beginners at the OS, and use standard tricks, well known bugs, and most of all, bad installation or management. As delivered, the system has some faults and bugs, but when used, the security may weaken due to installation of extra programs, changing file permissions, etc. Finding out new holes is something for 1) luck or 2) an expert. Experts generally know how to crack a system but don't find it challenging, worth the trouble (Nauta: e-mail interview).

Thus the criticism of technical justifications for hacking relies on the charge that the knowledge it produces, is very seldom, if ever, original. Whilst Cohen's view still allows for some benefits to stem from hacking in the sense that hackers may 'cut their horns' (sic) by gaining practical, if not particularly original, knowledge. The thrust of his argument is that such knowledge does not aid the development of computing and could be obtained in more orthodox ways. His criticism, along with Spafford's, who claims that the poor security of systems: "should be obvious to anyone studying software engineering", fails to resolve the problem of why, if such holes are well known, they are not fixed.

(ii) <u>The question of trust - the case of Robert Schifreen</u>

An important factor mitigating against increased cooperation with hackers is the practical consideration of being able to trust both the integrity and obedience of workers within an industrial/commercial setting. Tozer and Taylor were both at pains to emphasise the need for employers to be able to expect their

workers to only do the task given to them without allowing their curiosity to divert themselves. A 'vicious circle of trust'[9] can develop, however, whereby the only way to achieve specific knowledge of security issues is to indulge in illicit hacking activity, but the ownership of such knowledge subsequently debars the holder from being legitimately employed in the CSI.

One example of the general reluctance of the CSI to cooperate with, or to employ, hackers is given by 'smb', a U.S. security consultant, His reason why hackers' knowledge is not better used by the computing establishment is:

> Because they can't be trusted. I'm perfectly serious - would you hire someone for a sensitive position without good evidence that they weren't going to abuse their position? The hackers are either directly criminal, in which case you'd be a fool to hire them, or they're simply demonstrating a great deal of immaturity. In that case, why do you think they'll grow up if they get a new job? ... I'm not speaking in absolutes, of course. Circa 20 years ago, when I was working for a university computer center, I was faced with two students engaging in questionable activities. A brief investigation showed that both primarily wanted access to computing - but one of them was doing some fairly dubious things with his access. We turned that case over to the dean, and hired the other (Smb: e-mail interview).

These examples show that in previous times, hackers were valued for their technical ability and less concern was shown to such issues as trust or formal education in programming methods. With the more widespread dispersal of computers within the business world there has been a disproportionate increase in antipathy towards hackers, considering the act itself has remained constant. Dr Taylor gave the following explanation of his lack of trust for hackers:

> Well, it's the old, old story, if you employ someone who is close to your system security who is known to have a sort of

[9] c.f. Appendix 2 for a full account.

> criminal background or past criminal background, you don't know what they're going to do in terms of passing on information to third parties, because criminals have the wrong sort of information networks ... there's just this fear that they're going to pass to some of their friends, associates and so on, the information to hack into a system or some information they extracted out of it. If you let a hacker look around your system, they're bound to look into all sorts of confidential information like company plans for the next five years, which are on most big computers. It's the fact that they can't be trusted (Dr Taylor: Knutsford interview).

Despite the fact that hackers have at least a potentially useful role in the elimination of security holes, the issue of legitimacy mitigates against cooperation between the CU and the CSI. There are pragmatic considerations of whether hackers should be trusted with access to a company's systems, such as the possible litigious ramifications resulting from allowing known hackers access to systems that might subsequently be damaged. Mercury highlights the 'cover your back' type of approach to security, which arguably concentrates more upon fulfilling institutional and legal expectations than it seeks the best possible technical fix to a given security weakness. He describes how:

> I once sent out letters to hospitals offering my services. I included a xerox of an article about lax computer security in hospitals. Having been employed by a local software supplier to these hospitals, I was able to identify a couple of obvious examples. No takers. One system manager told me that it might be true that I knew more about computer security than a Big Eight Accounting Firm. 'But they bring other things to the table', he said. He meant that if he got an expensive audit from a Big Eight Firm and someone died anyway, he would be covered from liability (Mercury: e-mail interview).

Apart from the issue of trust, there is also the question of keeping the innate curiosity of a hacker in check. Both Dr Taylor and Mr. Tozer emphasised that in a commercial setting one of the most

important requirements they demand from their workers is a discipline to strictly follow instructions, and that they did not believe hackers would have such discipline. Thus Mr Tozer stated that:

> If these people aren't layabouts, if they've been looking for jobs, then the industry is desperate for people who have a good discipline and good technical ability. But have they got good discipline? In other words, could you ever use a hacker to do a proper job or would he want to go off on his own and do what he wants to do ... I think it must be a lack of discipline somewhere. You tell someone to go away and write a program to do something, not to do part of it and not to do all of it plus a bit more ... (Hawarden interview).

Finally, Prof Spafford is noted within the internet community for his more acerbic articulation of the belief that there should be minimal cooperation between those who are professionally responsible for the security maintenance of systems, and hackers.

> Everyone I know in major corporations, when faced with a choice between: a) a student whose resumé brags about all the machines he's broken into over the network; or b) a student whose resumé lists courses in cryptography, law, and software engineering would hire (b) and avoid (a) like the plague. If someone has already demonstrated a contempt for privacy and property rights, why would you want to hire them into a sensitive position working with important company data? It's like hiring a confessed arsonist to install fire alarms, or hiring an admitted paedophile as a teacher (Prof Sapfford: e-mail interview).

Robert Schifreen was arrested in 1984 for breaking into the Duke of Edinburgh's electronic mail account, the case and its subsequent publicity providing impetus for the subsequent drafting of the Computer Misuse Act of 1990. He now owns a computer-magazine publishing firm, and speaks at conferences, disseminating information about hacking in a guide that he has published. His actual security consultancy is more limited than he would wish or

had originally planned; reinforcing the points previously made about lack of hands-on knowledge in computer security. His experience illustrates the antagonism between the CSI and the CU and is a specific example of the subsequent lack of trust that exists between the two. It is of particular interest because he has had such direct and "test-case" status in the field of computer security and the "establishment's" attempts to deal with it. He is possibly the most famous example of the blurred division between the CU and the CSI referred to in journalistic language as, "the poacher turned game-keeper".

Acknowledging that CSI figures are often hostile to and denigrate the usefulness of hacking knowledge, Schifreen relates how he sometimes finds it difficult to find a receptive audience for his expertise:

> which is why I tend to speak at conferences and put things in writing rather than act as a consultant and go and talk to people face-to-face, or go and look at their computer systems and say "I wouldn't do that if I were you". Because yes, I can understand their reticence. They'll come and talk to me and ask me questions, general questions, nothing too specific, but there's a lot of knowledge out there that's either wrong or incomplete or non-existent and if I can scratch the surface and try and educate people, then I'll try and do so (Schifreen: London interview).

Thus, Schifreen's account of his reception within the CSI emphasises the willingness of firms to listen to general warnings concerning security weaknesses, yet a lack of trust and reluctant to accept detailed technical help from someone carrying the label of 'hacker'.

5.6 CONCLUSION

This chapter set out to analyse the following main issues: the extent to which security weaknesses exist; the reasons they are not eliminated; and the potential role of hackers in providing security expertise. Evidence from both the qualitative and quantitative fieldwork has illustrated the depth of security weaknesses within computing. The statistical analysis has further suggested that reported weaknesses are likely to be understated in official reports.

The reasons why security flaws are not eliminated are linked to the factors that give rise to their existence in the first place. Both the qualitative and quantitative fieldwork evidence illustrate the two main causes of the existence of security weaknesses and the accompanying gap between programming's achievements and expectations; computing's relatively immature status as an industry and the pressures caused by the demands of marketing. The former gives rise to a scarcity of theoretical knowledge surrounding computer security. Thus the fieldwork recounted various calls for more 'hands-on' experience of security from which theory can be garnered. The commercial pressures that exacerbate weaknesses have also been recounted. The CSI figures emphasise their frustration at the lack of adequate provision made for security as a result of the commercial desire to avoid expense, whilst both the CU and CSI perceive poor levels of security, in some instances at least, as being evidence of apathy.

Hawks and doves respond differently to the fact that the nature and motivation of a computer intruder is hidden from those in charge of the system. Whereas such figures as Taylor, Tozer and Jones, use the unknown nature of intruders as an argument for having to treat all intruders as if they were criminals, Herschberg emphasises that the ethical desire to castigate is supplanted by the technical responsibility of system operators to maintain their systems' security. It behoves operators to accept help from whatever quarter it is offered from. This failure to fully address

computing's inherent security and operational weaknesses is what leads Herschberg to bemoan the computing industry's aversion to, and subsequent lack of, practical 'hands-on' security knowledge. It is the same failure, however, that also leads hawkish figures to press for the stigmatisation of hackers and their subsequent exclusion from influence within computing.

This chapter's analysis of the software crisis is significant for the way in which it describes the potential role hackers have in helping to provide better security, and also its relevance to the origins of the marginalisation of hackers within computing. Hackers' potential to provide useful information about security weaknesses is likely to remain, despite criticism from the hawks, due to the fact that there are always likely to be difficulties in attempting to anticipate the possible sources of security breaches. Hackers' hands-on approach to testing is a practical way of providing that information. In addition, it is likely that hacking will survive in some form or another, considering it exhibits aspects of the craft qualities of programming that have not been (and are unlikely to be) eliminated as programming develops towards more science-based methods. Despite the fact that these qualities have not been totally eliminated, the pressures within computing to adopt more rigorous methods of software development have contributed to the marginalisation of the more craft-based hacker-type programmers. This has provided the origin of the 'them and us' scenario: the subject of the next chapter.

Chapter 6 - 'Them and us'

6.1 INTRODUCTION

6.2 BOUNDARY FORMATION - 'THEM AND US'
6.2.1 The evidence - Hawkish strength of feeling

6.3 REASONS FOR 'THEM AND US'
6.3.1 Ethical differences between the CSI and CU
6.3.2 The fear of anonymity

6.4 THE ETHICAL BASIS OF THE 'THEM AND US' SCENARIO
6.4.1 Blurred and vestigial ethics
6.4.2 Industry examples of blurred ethics
6.4.3 Technology and ethics

6.5 BOUNDARY FORMATION - ROLE OF THE MEDIA

6.6 BOUNDARY FORMATION PROCESS AND THE USE OF ANALOGIES

6.7 THE PROJECT OF PROFESSIONALISATION
6.7.1 Creation of the computer security market and professional ethos
6.7.2 Witch-hunts and hackers
6.7.3 Closure - the evolution of attitudes

6.8 CONCLUSION

6.1 INTRODUCTION

> *Hackers are like kids putting a 10 pence piece on a railway line to see if the train can bend it, not realising that they risk derailing the whole train* (Mike Jones: London interview).

The technical objections of the hawks to hacking, which reject the argument advocating cooperation with hackers, are supplemented by their ethical objections to the activity, explored in this chapter. Previous chapters have shown that there is some interplay and contact between the hacker community and the computer security industry, as well as the more subsidiary group: the academics[1]. The much more common relationship between hackers and the computer security industry, however, is the thinly-veiled or open hostility evident in the opinions of the hawks.

This chapter examines the basis of this hostility. The groups' contrasting ethical stances are highlighted, and their origins explained. The technical evolution of computing is shown as creating new conditions that demand ethical judgements to be made with respect to what constitutes ethical use of computer resources. The CU and the CSI have different ethical interpretations that are expressed in a process of debate. This debate then becomes part of a boundary forming process between the two groups. Two identifiable influences upon such ethical judgements are the age of the person making the judgement, and the extent to which technology plays a part in the situation about which an ethical judgement has to be made.

Elements of the CSI and the CU stand in identifiable opposition to each other. This chapter shows how this opposition is maintained and exacerbated as part of a boundary forming process. Ethical

---

[1] Thus Eric Coggans and Robert Schifreen (as well as several other hackers encountered in the fieldwork) have started their own computer firms; Professor Herschberg has contacts with and produces interaction between hackers and the security industry by means of his consultancy work, and the authorised and unauthorised (in the case of accepting a documented hack in lieu of a dissertation) use of students to test systems.

differences between the two groups are espoused, but examples are given of the extent to such differences are still in a process of formation within computing's nascent environment. Thus the type of mentality within the CU that fails to accept any ethical implications from phone-phreaking or hacking is sharply opposed by the CSI, whose typical sentiment is that computer users such as hackers have forgotten "that sometimes they must leave the playpen and accept the notion that computing is more than just a game" (Bloombecker 1990: 41). This contention that hackers have failed to psychologically "come out of the playpen" is illustrative of some of the marked ethical differences between the two groups.

This chapter, however, draws attention to examples of the more ambiguous and blurred ethical situations within computing, and how an on-going process of negotiation, group differentiation and boundary formation, is required to maintain such differences between the groups. The ethical complexities surrounding computing are becoming increasingly important as it becomes a more prevalent aspect of everyday life. The CSI, as a part of a dominant social constituency of business and political interests, is involved in a process of attempting to impose its interpretation of such ethical issues upon computing. Advocates of different ethical approaches find themselves increasingly separated by moral boundaries that have become codified into professional regulations and government legislation.

The "them and us" scenario caused by the contrasting ethical stances is fuelled by the media's portrayal of hackers as unethical outsiders. The most obvious manifestation of this is the evolution of attitudes held towards hackers by the dominant social constituency. The 'true hackers' of MIT were active from the late 1950's and were instrumental in the development of both hardware and software, whereas hackers are now largely perceived as a problem to be legislated away. This evolution in perceptions is simultaneously a result of the emergence of the CSI as a constituency, and a causal factor in that development. To illustrate the process of boundary formation we note comparisons of the debate surrounding Robert

Morris Jr's intrusion into the internet system with the language and attitudes displayed during the Salem Witch trials (Dougan and Gieryn 1988). The press, in particular, has been particularly active in the process of stereotyping and sensationalising hacking incidents, the process helping to produce a deviant group status for hackers.

The chapter also includes analysis of one of the most interesting aspects of the boundary forming process between the CSI and the CU, namely, the way in which physical comparisons are made between situations that arise in computing and the real world. These metaphors are used as explanatory tools and also in the production and maintenance of the value systems that separate the two groups. The physical analogies used seem to fulfil both of these functions. They allow what would otherwise be potentially complicated technical and ethical questions to be approached in a more manageable and everyday manner, yet they also contribute directly to the formation of ethical boundaries due to their particular suitability as a means of sensationalising hacking issues.

Public commentators such as Gene Spafford have made various polemical statements of what hacking and its implications are: employing a hacker, is like making 'an arsonist your fire chief, or a paedophile a school teacher.' The actions of hackers are thus forcefully taken out of the realms of 'cyberspace' and reintroduced into the concrete realm of threatening real world situations. If the comparison is accepted, then the danger and harm to be suffered from such actions are more readily understood and feared, and hackers as a group may then be effectively viewed as moral pariahs. With reference to Woolgar's (1990) attempt to link computer virus stories with the prevalence of 'urban/contemporary legends', it can be pointed out that the physical analogies used by the CSI in discussions of computer ethics emphasise the transgressive 'breaking and entering' qualities of hacking[2]. In contrast, the CU reject such dramatic analogies and prefer to emphasise the intellectual and pioneering qualities of hacking which we will subsequently analyse

[2] Fear of boundary transgression is vividly portrayed in such urban legends as 'The Mexican Dog' and 'The Choking Doberman', c.f. Woolgar (1990).

with respect to their chosen analogies: comparisons of hacking's intellectual nature and frontier ethos to a game of chess and the Wild West, respectively.

6.2 BOUNDARY FORMATION - 'THEM AND US'

Dougan and Gieryn (1988), like Meyer and Thomas (1990), have compared the process of boundary formation within computing with the historical examples of formalised witch trials. This is an extreme process of 'boundary formation' whereby groups differentiate themselves by marginalising other groups thereby establishing their own identity. "Witch hunts" occur in periods of social transition and we have seen in Chapter 3 that IT is undergoing a period of social change. The economic order is attempting to impose property relations upon information, yet its changing nature undermines its properties as a commodity.

Computer counter-cultures are increasingly perceived as a threat to the establishment's ability to control technology for its own purposes. The initial awe and even respect with which hackers were originally viewed as 'technological wizards' has given way to the more frequent hawkish perception that they are 'electronic vandals'. Dominant social groups initially mythologise and then stigmatise peripheral groups that do not share their value-structure. In the case of hackers, this tendency has been exacerbated by the fear and ignorance encouraged as a result of hacking's covert nature and the difficulties of documenting the activity.

Dougan and Gieryn (1988), amongst others, point out that such concepts of deviancy have a function. Put simply, a community only has a sense of its community status by knowing what it is not. Distancing themselves from outsiders helps members within that group feel a sense of togetherness. Furthermore, cultures that emphasise certain values over others will tend to label as deviant those activities which threaten its most prized value. In the particular case of hackers, their stigmatisation and marginalisation has occurred because they have threatened, with their information-

sharing culture, one of the basic crutches of the capitalist order: property rights. The facilitating feature of the boundary forming process between the CU and the CSI is the sense of otherness and lack of affinity with which they confront each other: the "them and us" scenario.

6.2.1 The evidence - hawkish strength of feeling

Direct access to the debate between the CSI and CU can be obtained by looking at examples of e-mail correspondence known as 'flames'. These are strongly worded, and often insulting electronic mail messages. They serve to illustrate the antagonism that exists between the CSI and CU. The following are examples of the expressions used on e-mail to describe hackers and hacking:

> I am for making the penalties for computer trespass extremely painful to the perpetrator ... Most administrators who've had to clean up and audit a system of this size probably think that a felony rap is too light a sentence. At times like that, we tend to think in terms of boiling in oil, being drawn and quartered, or maybe burying the intruder up to his neck in an anthill (Bob Johnson: RISKS electronic digest, 11:32).

> electronic vandalism (Warman: e-mail interview).

> Somewhere near vermin i.e. possibly unavoidable, maybe even necessary pests that can be destructive and disruptive if not monitored (Zmudsinki e-mail interview).

> Mostly they seem to be kids with a dramatically underdeveloped sense of community and society (Bernie Cosell: e-mail interview).

Opposition to hacking practices has become increasingly non-specific and moralistic, an example being Spafford's argument that using hackers' knowledge on a regular basis within the computer

security industry is equivalent to employing a known arsonist as your fire-chief, a fraudster as your accountant, or a paedophile as your child-minder. The technical insights that they could provide or could be derived as a by-product of their activities become subordinate to the need to express opprobrium against the morality of the actions themselves. The language of blame and morality is consistently used by hawkish members of the CSI to refer to hackers in what they would argue is a process of 'blame displacement'. The CSI are accused of using moral condemnation as a means of deflecting any responsibility and blame for security breaches that might be attached, not just to the perpetrators of intrusions, but also their victims. As Herschberg said:

> The pseudo-moral arguments and the moralistic language certainly cloud the issue in my view. I think it obscures the fact that system owners or system administrators have a moral duty to do at least their level best to stop penetrations. They are very remiss in their duty, they couldn't care less and therefore at least, there is quite an understandable tendency to blame the penetrator rather than blaming themselves for not having taken at least adequate counter measures, in fact in some cases counter measures have not been taken at all ... if it is proved to you that you haven't done your homework, then you almost automatically go into a defensive attitude which in this case, simply amounts to attacking the hacker, blaming him morally, heaping opprobrium on his head ... yes, the fear factor is involved (Herschberg: Delft interview).

This undercurrent of moral censure was a recurrent quality of the field-work interviews with members of the CSI, for example:

> I've been in this game ... this is my 36th year, in the interests of hacking as a whole I think hacking is something which is derogatory; to be played down, to possibly in fact, be treated as a minor form of criminal activity ... the last thing you want to do is to make hackers into public figures; give them publicity. I think it needs to be played down when it occurs, but it

shouldn't occur ... I wouldn't have them, no, under any circumstances (Taylor: Knutsford interview).

Dr Taylor and others interviewees, involved in the provision of computer security, had had surprisingly little direct contact with hackers. I asked him about this lack of direct contact/interplay and his perceptions of the motivations of hackers:

> Well, there shouldn't be [any interplay] because the industry doesn't want to hear about hackers and certainly doesn't want to see the effects of what they do ... To me I'm not concerned with what the hacker does, I'm more concerned with keeping him out to start with ... You've talked to what are called the more ethical members of the hacking community for whom it's an intellectual challenge, but there are in fact people who are psychopaths, and Doctor Popp[3] is one of these, where they just want to level a score with society which they feel has been unfair to them ... A chap called Whitely has just gone to prison for four years for destroying medical data at Queen Mary's hospital, London. He just destroyed utterly and he wasn't just a hacker that was browsing, he was a psychopath almost certainly (Taylor: Knutsford interview).

In contrast, and as an illustration of the negative perceptions each groups has of the other, a hacker, Mofo, argues that psychotic tendencies are not the sole preserve of the hacking community:

> my experience has shown me that the actions of 'those in charge' of computer systems and networks have similar 'power trips' which need be fulfilled. Whether this psychotic need is developed or entrenched before one's association with computers is irrelevant. Individuals bearing such faulty mental health are present in all walks of life. I believe it is just a matter of probability that many such individuals are

[3] Joseph Lewis Popp: he was charged in January 1990 with using a trojan horse hidden within a diskette to extort money from recipients whose systems had subsequently become infected. The trial did not come to court, however, because his defence argued that he was mentally unfit to stand trial. They described how he had taken to putting hair curlers in his beard and wearing a cardboard box on his head in an apparent attempt to protect himself from radiation.

somewhat associated with the management of computers and networks [as well as intrusion into computer systems] (Mofo: e-mail interview).

Taylor is wary of the damage to computing that greater publicisation of hacking could cause, yet as the above reference to Dr Popp and Nicholas Whitley shows, ironically, he seemed to be dependent upon the most publicised cases of hacking for his perceptions of hackers. A further argument that prevents the CSI accepting hackers as potentially useful fault-finders in systems is the simple charge that without the existence of hackers in the first place, there would be very little need for extensive security measures. Even if hackers are of some use in pointing out various bugs in systems, such a benefit is outweighed by the fact that a large amount of computing resources are 'wasted' on what would otherwise be unnecessary security measures. For example, Dr Taylor's view is that:

> hacking is a menace that stops people doing constructive work ... A lot of money get's spent today on providing quite complex solutions to keep ahead of hackers, which in my view should not be spent ... They're challenging the researchers to produce better technical solutions and they're stimulating the software service industry which provides these solutions and makes money out of it. But you answer the question for me, what's that doing for society? (Taylor: Knutsford interview).

Thus one reason for the use of moral language is in order to displace blame from those in charge of the systems where security is lax, to those who have broken that lax security. Irrespective of the state of security of systems, there is a project of group formation whereby those who implement computer security wish to isolate and differentiate themselves from the CU, in a process that highlights the inherent differences that exist between the two groups. This project is vividly illustrated in the following excerpt from the keynote Turing Award acceptance speech given by Ken Thompson:

> I have watched kids testifying before Congress. It is clear that they are completely unaware of the seriousness of their acts. There is obviously a cultural gap. The act of breaking into a computer system has to have the same social stigma as breaking into a neighbor's house. It should not matter that the neighbour's door is unlocked. The press must learn that misguided use of a computer is no more amazing than drunk driving of an automobile (Thompson 1984: 763).

This degree of sentiment was consistently expressed amongst some of the most prominent and accomplished of those figures from the computer security industry who were generally opposed to hackers:

> Unfortunately ... it is tempting to view the hacker as something of a folk hero - a lone individual who, armed with only his own ingenuity, is able to thwart the system. Not enough attention is paid to the real damage that such people can do...when somebody tampers with someone else's data or programs, however clever the method, we all need to recognise that such an act is at best irresponsible and very likely criminal. That the offender feels no remorse, or that the virus had unintended consequences does not change the essential lawlessness of the act, which is in effect breaking-and-entering. And asserting that the act had a salutary outcome, since it led to stronger safeguards, has no more validity than if the same argument were advanced in defense of any crime. If after experiencing a burglary I purchase a burglar alarm for my house, does that excuse the burglar? Of course not. Any such act should be vigorously prosecuted (Parrish 1989).

Several of the above quotations are notable for their heavy reliance upon the visual imagery of metaphors comparing the ethical issues arising from computing with real-world situations, a topic that will be looked at shortly.

6.3 REASONS FOR 'THEM AND US'

6.3.1 Ethical differences between the CSI and CU

Having identified the strength of feeling of hawkish views of hacking, this section explores the ethical basis of that antagonism. The following quotation from a member of the CSI illustrates the stark difference between the ethical outlooks of certain members of the computing constituency. Elements of the CSI vehemently oppose the "playpen attitude" advocated by elements of the CU. Presupposing that no harm is done, hackers tend to believe that it is not wrong to explore systems without prior permission, whilst those concerned with the security of those systems would characterise such a belief as offensive:

> Just because YOU have such a totally bankrupt sense of ethics and propriety, that shouldn't put a burden on *me* to have to waste my time dealing with it. Life is short enough to not have it gratuitously wasted on self-righteous, immature fools...If you want to 'play' on my system, you can ASK me, try to convince me *a priori* of the innocence of your intent, and if I say "no" you should just go away. And playing without asking is, and should be criminal; I have no obligation, nor any interest, in being compelled to provide a playpen for bozos who are so jaded that they cannot amuse themselves in some non-offensive way (Cosell CUD 3:12).

When we examine the factors underpinning the CSI's and CU's contrasting ethical interpretations we find an important feature is the tendency of the CSI to denigrate, or devalue the ethics articulated by hackers. Bob Johnson, a Senior Systems analyst and Unix System Administrator at a US military installation criticises the justifications used by hackers as an example of the modern tendency to indulge in "positional ethics". Referring to the Internet worm case he states:

> The majority of people refuse to judge on the basis of "right and wrong". Instead, they judge the actions in terms of result, or based on actual damages, or incidental damages or their own personal ideas. In my mind, Morris was WRONG in what he

did, regardless of damages, and should therefore be prepared to pay for his deeds. Many others do not suffer from this "narrow frame of mind". By the way, positional ethics is the same line of reasoning which asks, "When would it be right to steal a loaf of bread?" I believe that the answer is "It may someday be necessary, but it's never right" (Bob Johnson: e-mail interview).

The "hawkish" elements of the CSI are unequivocal in their condemnation of hacking and its lack of ethics. They argue that the lack of ethics shown by hackers is indicative of a wider societal decline. Thus Smb characterises the alleged degeneration of the average persons ethics, not as a breakdown in morality, but rather as a spread of amorality: "I'm far from convinced that the lack of ethics is unique to hackers. I think it's a societal problem, which in this business we see manifested as hacking. Amorality rather than immorality is the problem" (Smb: E-mail interview). Similarly, Bob Johnson argues that:

> In a larger sense, I view them [hacking and viruses] as part of the same problem, which is a degeneration of the average persons ethics - i.e. integrity and honesty. There's a popular saying in America - 'You're not really breaking the speed limit unless you get caught. I believe an ethical person would neither break into systems, nor write viruses (Bob Johnson: e-mail interview).

Cosell takes this argument further, the "degeneration of the average person's ethics" is applied to a loss of respect by hackers for property rights:

> The issue here is one of ethics, not damages. I'll avoid the "today's children are terrors" argument, but some parts of that cannot be avoided: the hackers take the point of view that the world at large OWES them amusement, and that anything they can manage to break into is fair game [an astonishing step beyond an already reprehensible position, that anything not completely nailed down is fair game] (Cosell: e-mail interview).

A study into social and business ethical questions was carried out by Johnston and Wood (1985, cited by Vinten 1990) for the British Social Attitudes Survey. Apart from their major conclusion that the single most important factor influencing the strength of people's ethical judgements was age, it seems difficult to point to clear ethical boundaries and guide-lines in relation to many of the situations that arise in the modern world, especially in the realms of business. Thus in his summary of the report Vinten describes how: "In situations ranging widely from illegitimate tipping of dustmen to serious corruption, no clear-cut boundaries emerged as between 'right' and 'wrong' ... Sub-group variation was greatest where situations were complicated by motivation questions, and by being remote from everyday experience" (Vinten 1990: 3). Hacking fulfils both of these criteria.

The advent of "virtual reality" or "cyberspace" tends to divorce computing from "everyday experience". This leads directly to an ambiguous ethical status for many computing situations and a concomitant need to assert ethical standards by the dominant social constituency if it is to succeed in exerting control over computing. Vinten's study of computer ethics (1990) points out that ethical judgements tend to be harsher, the older the person making the judgements. Members of the CSI consistently have strongly critical views of the ethical stance taken by hackers. They tend to be older than hackers, having been involved with computers, as a career, for many years. Hackers, in contrast, tend to use computers more as a hobby and may hack in order to gain access to systems which their youth precludes them from obtaining access to by legitimate means. This age difference is perhaps one reason why there are such fundamental differences in the ethical outlook of members of the CSI and CU[4].

6.3.2 Fear of Anonymity

[4] c.f. Appendix 1's summary of the fieldwork's statistical evidence of the age factor.

One of the common themes that stems from the CSI's perception of hackers is their tendency to assume the worst intent behind the actions of intruders, a tendency encouraged by the fact that hacking is intrinsically anonymous:

> There is a great difference between trespassing on my property and breaking into my computer. A better analogy might be finding a trespasser in your high-rise office building at 3 AM, and learning that his back-pack contained some tools, some wire, a timer and a couple of detonation caps. He could claim that he wasn't planting a bomb, but how can you be sure? (Cosell: e-mail interview).

Another vivid example of the doubt caused by the anonymity of hackers is the comparison below made by Mike Jones of the DTI's security awareness division. I pointed out that many hackers feel victimised by the establishment because they believe it is more interested in prosecuting them than patching up the holes they are pointing out with their activity. Jones accepted that there was prejudice in the views of the CSI towards the CU. That prejudice, however, is based upon the **potential** damage that hackers can cause. Even if there is no malicious intention from the hacker, suspicion and doubt as to what harm has been done exists:

> Say you came out to your car and your bonnet was slightly up and you looked under the bonnet and somebody was tampering with the leads or there looked like there were marks on the brake-pipe. Would you just put the bonnet down and say "oh, they've probably done no harm" and drive off, or would you suspect that they've done something wrong and they've sawn through a brake-pipe or whatever... say a maintenance crew arrived at a hanger one morning and found that somebody had broken in and there were screw-driver marks on the outside casing of one of the engines, now would they look inside and say "nothing really wrong here" or would they say, "hey, we've got to take this engine apart or at least

look at it so closely that we can verify that whatever has been done hasn't harmed the engine" (Jones: London interview).

These two quotations proffer an important explanation of the alleged paranoid and knee-jerk reactions to hacking activity from the computing establishment. The general prejudice held by the CSI towards the CU is heightened by the anonymous quality of hacking. The anonymity encourages doubts and paranoia as a result of being unable to assess the motivation of intruders and the likelihood that any harm that has been committed will be difficult to uncover.

In addition to these points, the anonymity afforded by Computer Mediated Communication (CMC) encourages hackers to project exaggeratedly threatening personalities to the outside world and media. Barlow (1990) describes meeting some hackers who had previously frightened him with their aggressive e-mail posturing. When Barlow actually came face to face with two of the hackers they:

> were well scrubbed and fashionably clad. They looked to be as dangerous as ducks. But ... as ... the media have discovered to their delight, the boys had developed distinctly showier personae for their rambles through the howling wilderness of Cyberspace. Glittering with spikes of binary chrome, they strode past the klieg lights and into the digital distance. There they would be outlaws. It was only a matter of time before they started to believe themselves as bad as they sounded. And no time at all before everyone else did (Barlow 1990: 48).

The anonymity afforded by CMC thus allows hacking culture to indulge in extravagant role-playing which enhances the perception of it in the eyes of outsiders as being a potentially dangerous underground movement. Hacking groups generally choose colourful names such as "Bad Ass Mother Fuckers, Chaos Computer Club, Circle of Death, Farmers of Doom"[5], and so on.

6.4 THE ETHICAL BASIS OF THE 'THEM AND US' SCENARIO

---

[5] Sterling 1993: 95

6.4.1 Blurred and vestigial ethics

> *Cracking, virus writing, and all the rest, fall into the realm of possibility when dealing with intelligent, curious minds. The ethics of such things come later. Until then, users of computers remain in this infancy of cracking, etc.* (Kerchen: e-mail interview).

The ethical edges demarcating legal and illicit acts have a higher tendency to be blurred whenever technology has a significant presence in the context of the act. The acts of such figures as Captain Crunch have been received with a combination of admiration and condemnation. Opposition to attempts to commodify and institutionalise informational property relations can exist in such rebellious manipulations of technology; but also more 'respectably' in the intellectual and political platforms of such figures as Richard Stallman and the League for Programming Freedom. Activities involving the use of computers have given rise to a number of qualitatively new situations in which there is a debate as to whether the act in question is ethical or not. These activities tend to centre upon such questions as whether the unauthorised access to and/or use of somebody's computer, system, or data can be adequately compared to more traditional crimes involving the physical access or manipulation of material objects or property.

An example of such ambiguity is the fact that whereas the idiosyncratic behaviour of the early hackers of MIT was benignly tolerated now hacking is portrayed in the press as having evil associations and is subject to legal prosecution. This apparent change in social values has occurred despite the fact that the motivations and lack of regard for property rights associated with hacking have remained constant over time. Examples of the previously ad hoc morality with respect to computers abound. The first generation MIT hackers engaged in such illicit activity as using equipment without authorisation (Levy 1984: 20), phone phreaking (pg 92), unauthorised modification of equipment (pg 96) and the

circumvention of password controls (Pg 417)[6]. Bloombecker gives the example of how authority's reaction to the behaviour of small school children may represent society's ambivalent response to the computing activities it originally encourages. Definitive ethical judgements can prove difficult to make in certain situations:

> Think of the dilemma expressed unknowingly by the mathematics teacher who spoke of the enthusiasm her 9 and 10-year-old students exhibited when she allowed them to use the school's computers. "They are so excited" she said, "that they fight to get onto the system. Some of them even erase others' names from the sign-up lists altogether". The idea that this was not good preparation for the students' moral lives seemed never to have occurred to her ... Unfortunately, both for society and for those that need the guidance, there is no standard within the computer community to define precisely when the playing has got out of hand. If a student uses an hour of computer time without permission, one university computer department may consider it criminal theft of service, while another views it as an exercise of commendable ingenuity (Bloombecker 1990: 42).

This ambiguous ethical status of some computing activities is due to the relatively recent advent of computing as an area of human endeavour; this has led to a lack of readily agreed-upon computing mores: "Indeed, if we were to devise a personality test designed to spot the computer criminal, the first and most difficult task would be to create a task that did not also eliminate most of the best minds who have made computing what it is" (Bloombecker 1990: 39). There is the further complicating factor, that to some extent at least, society encourages "getting hooked" upon computing, since it is perceived as representing a beneficial outlet for intellectual endeavour. We now turn to more specific examples of computing's ethical complexity.

6.4.2 Industry examples of blurred ethics

[6] references taken from CuD 4.11

There is often a lack of agreement even amongst computer professionals as to what constitutes the correct procedures with which to confront certain research and educational issues within computing. A specific example of this lack of agreement is the debate caused by the publication of an article by Cohen, entitled "Friendly contagion: Harnessing the Subtle Power of Computer Viruses" (1991). In the article, Cohen suggests that the vendor of a computer virus prevention product should sponsor a contest encouraging the development of new viruses, with the provisos that the spreading ability of the viruses should be inherently limited, and that they should only be tested on systems with the informed consent of the systems owners. Spafford responded with the charge that: "For someone of Dr Cohen's reputation within the field to actually *promote* the uncontrolled writing of any virus, even with his stated stipulations, is to act irresponsibly and immorally. To act in such a manner is likely to encourage the development of yet more viruses "in the wild" by muddling the ethics and dangers involved" (Spafford 1991: 3). Furthermore, even the publication of "fixes" can be viewed in certain instances as an unethical act, leading to what has been previously described as the phenomenon of "security through obscurity". Spafford argues that: "We should realize that widespread publication of details will imperil sites were users are unwilling or unable to install updates and fixes. Publication should serve a useful purpose; endangering the security of other people's machines or attempting to force them into making changes they are unable to make or afford is not ethical" (Spafford 1990:12).

The disagreement over some of the ethical questions thrown up by hacking was also in evidence in the aftermath of the Internet Worm when a debate raged amongst computer professionals as to the ethical and technical implications of the event. The debate tending to support the above argument positing ethical sub-group variation and a general lack of clear-cut moral boundaries as typical of the modern ethical environment, especially when there are contrasting opinions as to the originating motivations behind specific

acts. Such a debate was reflected in the "Communications of the Association of Computing Machinery (ACM)" Forum of Letters, where even the ACM's president received quite strident criticism for his position indicated in the title of his letter: "A Hygiene Lesson", that the Internet Worm could be viewed as beneficial in so far as it increased awareness of security practices. The president's view was described by one contributor to the forum as, "a massive error in judgement which sends the wrong message to the world on the matters of individual responsibility and ethical behaviour ... [it] is inexcusable and an exercise in moral relativism" (Denning, Peter 1990: 523). Similarly, another writer illustrates the disparate nature of the feelings produced by the Internet Worm incident when he pointedly remarks:

> while Spafford praises the efficacy of the "UNIX 'old boy' network" in fighting the worm, he does not explain how these self-appointed fire marshals allowed such known hazards to exist for so long ... If people like Morris and people like him are the greatest threat to the proper working of the Internet then we face no threat at all. If, on the other hand, our preoccupation with moralizing over this incident blinds us to serious security threats and lowers the standards of civility in our community, then we will have lost a great deal indeed (Denning, Peter 1990: pp 526 +7).

6.4.3 Technology and ethics

Underlying some of these problems with ethics has been the tendency identified by Spafford (1990) to "view computers simply as machines and algorithims, and ... not perceive the serious ethical questions inherent in their use" (Spafford 1990: 12). Spafford points to the failure to address the end result of computing decisions upon people's lives, and hence the accompanying failure to recognise the ethical component of computing. As a result, he argues, there is a subsequent general failure to teach the proper ethical use of computers:

> Computing has historically been divorced from social values, from human values, computing has been viewed as something numeric and that there is no ethical concern with numbers, that we simply calculate values of 0 and 1, and that there are no grey areas, no impact areas, and that leads to more problems than simply theft of information, it also leads to problems of producing software that is also responsible for loss and damage and hurt because we fail to understand that computers are tools whose products ... involve human beings and that humans are affected at the other end (Spafford US interview).

This is due to the fact that often the staff of computer faculties are uncomfortable with the subject, or don't believe it's important. Their backgrounds are predominantly in mathematics or scientific theory and hence they don't adequately understand how practical issues of use may apply to computing. Spafford suggests that engineering provides a more appropriate model of computing than science in so far as it addresses the human as well as the scientific dimensions.

> Computer science is really, in large part an engineering discipline and that some of the difficulties that arise in defining the field are because the people who are involved in computing, believe it's a science and don't understand the engineering aspects of it. Engineers, for a very long time, have been taught issues of appropriateness and ethics and legality and it's very often a required part of engineering curricula ... computing is more than just dealing with numbers and abstractions, it does in fact have very strong applications behind it, a very strong real-world component (Spafford US interview).

The extent to which computing has a non-material dimension, however, constantly mitigates against Spafford's desire for computing to be ethically approached in a similar manner to an engineering discipline. There is a fundamental difference between

the 'real world' and the 'virtual world' of computing, and it is this difference which makes the literal transposing of ethical judgements from the former to the latter, difficult, if not untenable. The correct balance with which to transpose ethical judgements from one realm to another is debateable.

6.5 BOUNDARY FORMATION - ROLE OF THE MEDIA

This section debunks some of the sensationalising, demonising, and mythologising of hacking that has occurred with the recent spate of books, articles and television programmes dealing with the issue. It also corrects the overwhelming tendency of most of the writings on the subject of hacking to concentrate on the minutiae of the activities and life histories of hackers or their adversaries. Frequently, but superficially, deep-rooted psychological abnormalities are offered as explanations for hacking activity, whilst ignoring the ethical and political implications of those acts. The overall effect of the media portrayal of hacking, it could be suggested, is a continuation by other means of the CSI's project of stigmatisation and closure.

(i) 'Hacker best-sellers'

Two examples of the tendency towards sensationalism are The Cuckoo's Egg by Clifford Stoll and Cyberpunk by Hafner and Markoff. An example of the many uses of hyperbole in their choice and tone of language is their consideration of the issues at stake in the hiring of a hacker for security work. "But hire such a mean-spirited person? That would be like giving the Boston Strangler a maintenance job in a nursing-school dormitory" (Hafner and Markoff, 1991: 40). Both of these books made a large impact on the computing public and yet both seem self-indulgent in their reliance upon trivial and tangential details in the narration of different hacking episodes. In The Cuckoo's Egg, for example, we are given various descriptions of the author's girlfriend and seemingly

irrelevant details of their shared Californian lifestyle. In Cyberpunk, many unsubstantiated conjectures are made as to the state of mind of the hacker. Thus the authors write about Kevin Mitnick:

> When Kevin was three, his parents separated. His mother, Shelly got a job as a waitress at a local delicatessen and embarked upon a series of new relationships. Every time Kevin started to get close to a new father, the man disappeared. Kevin's real father was seldom in touch; he remarried and had another son, athletic and good-looking. During Kevin's high school years, just as he was getting settled into a new school, the family moved. It wasn't surprising that Kevin looked to the telephone for solace (Haffner and Markoff 1991: 26).

This somewhat arbitrary assignation of motivation leads the authors to label Kevin Mitnick as the "dark-side" hacker, whereas their analysis of Robert Morris, author of the Internet Worm, is much less condemning despite the fact the latter was responsible for much more damage and man-hours of data-recovery time.

(ii) Press and Television

The media faces, in its reporting of computer security issues, the perennial problem of how to report technical issues in a both accurate and entertaining manner. Generally, the media has tended towards reporting those stories that contain the highest degree of 'electronic lethality' and it has exaggerated the 'darkness' of hacking motives. For example, a Channel Four television documentary "Dispatches" entitled its investigation of hacking "The day of the Technopath", whilst the February 1991 edition of GQ magazine concerned the growth of virus writers in Bulgaria and was called "Satanic Viruses".

Along with the above two treatments of the computer security issue I will also look at a Sunday Correspondent article of the 17th December 1989 entitled "A Bug in the Machine" and part of the transcript of an episode of the U.S. current affairs/chat-show

programme, "Geraldo", for a sample of media treatments of the hacking issue. The television portrayals of the problem of computer security seem to be the most superficial and dependent upon sensationalising techniques. Newspaper and magazine articles to give relatively thorough and accurate technical descriptions of what it is to hack/write viruses but still make disproportionate use of 'dark-side' imagery[7].

"A Bug in the Machine"

This article is an example of the tendency of the press to concentrate upon the "sexy" elements of computer security stories. It contains a cynical description of Emma Nicholson M.P.'s unsubstantiated claims that hacking techniques are used for terrorist purposes by the European Green movement amongst others and her emotive description of hackers as: " ... malevolent, nasty evil-doers who fill the screens of amateur users with pornography" (Matthews 1989: 39). Yet whilst dispelling some of the alarmist tendencies of such claims, the example of a hacker chosen by the journalists is that of the "computer anarchist Mack Plug". Apart from making their own unsubstantiated claim that "Nearly all hackers are loners" (a contention refuted by my interviews with groups of Dutch hackers), their description of his hacking activity seems to deliberately over-emphasise the more "glamorous" type of hacking at the expense of describing the more mundane realities and implications of everyday hacking:

> At the moment he is hacking electronic leg tags. "I've got it down to 27 seconds" he says, "All you have to do is put a microset recorder next to the tag and when the police call to check you're there, you tape the tones transmitted by the tag and feed them on to your answering machine. When the cops call back again, my machine will play back those tones. I'll have a fail-safe alibi and I can get back to hacking into MI5 (Matthews 1989: 39).

---

[7] As shown with the title of Paul Mungo's article: "Satanic Viruses" (c.f. bibliiography)

Geraldo Programme[8]

On September 30th 1991, the Geraldo chat-show focused on hacking. It involved a presentation of various hacking cameo shots, one of which showed Dutch hackers accessing US Department of Defense computers with super-user status. The studio section of the show involved an interview with Craig Neidorf (alias Knight Lightning), who underwent a court case in the U.S. for having allegedly received the source code of the emergency services telephone computer programs. Also interviewed was Don Ingraham the prosecuting attorney in Neidorf's case.

Below I include excerpts from the dialogue that ensued as an example of the extent to which hacking is presented in the media in a superficial, trivialised and hyperbolic manner. In the introductory part of the show, excerpts from the film "Die Hard II" are shown in which terrorists take over the computers of an airport. The general tone of the show was sensationalistic with one of the guest hackers Craig Neidorf being repeatedly called the "Mad Hacker" by Geraldo and Don Ingraham consistently choosing emotive and alarmist language as shown in the following examples:

> Geraldo: Don, how do you respond to the feeling common among so many hackers that what they're doing is a public service; they're exposing the flaws in our security systems?
>
> Don: Right, and just like the people who rape a co-ed on campus are exposing the flaws in our nation's higher education security. It's absolute nonsense. They are doing nothing more than showing off to each other, and satisfying their own appetite to know something that is not theirs to know.

And on the question of the punishment of hackers:

---

[8] c.f. CuD 3:37

> I don't think they're being punished very much at all. We're having trouble even taking away their gear. I don't know one of them has done hard time in a prison. The book, Hafner's book on Cyberpunk, points out that even Mitnick who is a real electronic Hannibal Lecter ... did not get near any of the punishment that what he was doing entitled him to.

Finally, at the very end of the show, Geraldo asks Ingraham to give, in 30 seconds, a worst case scenario of what could result from the activities of hackers. To which he replies: "They wipe out our communications system. Rather easily done. Nobody talks to anyone else, nothing moves, patients don't get their medicine. We're on our knees."

Dispatches - "the day of the technopath"[9]

Emma Nicholson M.P. interviewed in the Dispatches programme, states, "A really good hacker could beat the Lockerbie bomber any day, hands down" and, "Perhaps only a small fraction of the population dislikes the human race, but they do, and some of them are highly computer-skilled".

The following is another example taken from the programme's voiced-over commentary:

> Until now the computer hacker has been seen affectionately as a skilled technocrat, beavering away obsessively in his den, a harmless crank exploring the international computer networks for fun. But today it's clear that any computer, anywhere, can be broken into and interfered with for ulterior motives. The technocrat has mutated to the technopath ... government and business are reluctant to admit that they're fragile and vulnerable to such threats, frightened of either the loss of public confidence or of setting themselves up as targets for the technopaths who stalk their electronic alleyways.

---

[9] Channel 4 Television, November 1989

6.6 BOUNDARY FORMATION PROCESS AND THE USE OF ANALOGIES

The previous sections of this chapter have established that the ethical issues surrounding computer usage are both complex and liable to fundamentally contrasting interpretations by the members of the CSI and the CU. The debate that subsequently occurs between the two groups has been shown as part of a boundary forming process by means of which both groups reinforce their own identities. This section analyses the way in which analogies are used within this process as both explanatory tools with which to examine some of the issues in the ethical debate over hacking, and also as a method of conveying the strength of opinion that is held.

The role of physical analogies in the ethical debate over security issues has already been illustrated with the CSI's use of them to express fears of the anonymous nature of the threat hackers pose. The general ease with which physical analogies are used and the strength of feeling behind them is vividly illustrated by Jerry Carlin's response to the question, "Have system breakers become the 'whipping boys' for general commercial irresponsibility with regard to data security?" He replied, "It's fashionable to blame the victim for the crime but if someone is raped it is not OK to blame that person for not doing a better job in fending off the attack!" (Carlin: e-mail interview) Sherizen was one of the few interviewees to refrain from using analogies in his discussion of hacking, contending that:

> Usually, arguing by analogy is a very weak argument. When it comes to discussing the law, non-lawyers often try to approach arguments this way. I don't think that we can go very far to determine appropriate behaviours if we rely upon analogies. What we need to develop are some social definitions of acceptable behaviour and then to structure "old law for new technologies." The physical analogies may help to score points in a debate but they are not helpful here at all (Sherizen e-mail interview).

The grey and indeterminate ethical quality of computing makes it difficult to establish such a code of 'acceptable behaviour', and it is in an attempt to do so that physical analogies are used. Goldstein (editor of Hacking magazine 'Phrack') explores the ethical implications of hacking by questioning the use of an analogy that likens hacking to trespass:

> Some will say ... 'accessing a computer is far more sensitive than walking into an unlocked office building.' If that is the case, why is it still so easy to do? If it's possible for somebody to easily gain unauthorised access to a computer that has information about me, I would like to know about it. But somehow I don't think the company or agency running the system would tell me that they have gaping security holes. Hackers, on the other hand, are very open about what they discover which is why large corporations hate them so much (Goldstein 1993).

The moral debate about hacking makes frequent use of such physical analogies of 'theft' and 'trespass'. The choice of the physical analogy reflecting the initial ethical position of the discussant and will be biased towards the point that the discussant is attempting to establish, and hence certain emotive images such as rape and burglary are repeatedly used.

(i) Property issues

Members of the CSI tend to emphasise the authorisation and access rights criteria relating to information. Such criteria are held to be fundamental to an ethical outlook on computing issues because of they stem from the basic belief that information and computer systems are the sole property of their owners, in the same way that

property rights exist in material objects. Physical analogies become a means to restrict the computer security debate: "to questions about privacy, property, possessive individualism, and at best, the excesses of state surveillance, while it closes off any examination of the activities of the corporate owners and institutional sponsors of information technology (the most prized 'target' of most hackers)." (Ross 1990: 83). This is a rather partisan interpretation of the role analogies play in the socially shaping boundary formation occurring within computing. A less controversial assessment, would be that in contrast to the CU, the CSI emphasises the property rights of system owners with its use of analogies that are often dramatic and vivid: "As far as the raison d'être for attackers, it is no more a valid justification to attack systems because they are vulnerable than it is valid to beat up babies because they can't defend themselves. If you are going to demonstrate a weakness, you must do it with the permission of the systems administrators and with a great deal of care" (Cohen: e-mail interview).

The difficulty faced with analogies that seek to emphasise the way in which hacking tends to transgress property rights, centres upon what we have already seen as the increasingly immaterial aspects of information and which is also shown in Chapter 7 to create various problems for drafting effective computer misuse legislation: "copyability is INHERENT in electronic media. You can xerox a book but not very well and you don't get a nice binding and cover. Electronic media, video tape, computer discs etc., do not have this limitation. Since the ability to copy is within the nature of the media, it seems silly to try to prevent it" (Mercury: e-mail interview). Software copying is an example of how duplication within computing is inherently more easy than with physical commodities: copyability is intrinsic to the medium itself. For example, Maelstrom contends that he: "can't remember a single analogy that works. Theft is taking something else that belongs to someone without his/her permission. When you pirate you don't steal, you copy" (Maelstrom: e-mail interview). Similarly, in the case of cracking:

> In absolutely no case can the physical analogies of 'theft' and 'trespassing' be applied in the matter of computer system 'cracking'. Computers are a reservoir for information expressed in bits of zeroes and ones. Homes and property have things far more intrinsically valuable to harbour. Information protected properly whilst residing on a system is not at issue for 'theft'. Encryption should have been a standard feature to begin with and truly confidential information should not be accessible in any manner via a remote means (Tester: e-mail interview).

(ii) Analogies - breaking and entering

In order to emphasise the potential harm threatened to systems by anonymous intruders the physical analogies used tend to concentrate upon the fear and sense of violation that tend to accompany burglaries. The dispute between the CSI and the CU as to whether it is ethical to break into systems is most often conducted with reference to the analogy of breaking and entering into a building. Because of the divergence between the real world and cyberspace, however, even such a simple analogy is open to varying interpretations: "My analogy is walking into an office building, asking a secretary which way it is to the records room, and making some Xerox copies of them. Far different than breaking and entering someone's home" (Cohen: e-mail interview).

Cosell presents the following scenario with which he attempts to frame the ethical issues surrounding hacking:

> Consider: it is the middle of summer and you happen to be climbing in the mountains and see a pack of teenagers roaming around an abandoned-until-snow ski resort. There is no question of physical harm to a person, since there will be no people around for months. They are methodically searching EVERY truck, building, outbuilding, shed etc., trying EVERY window, trying to pick EVERY lock. When they find something they can open, they wander into it, and emerge a while later. From your vantage point, you can see no actual evidence of any theft or vandalism, but then you can't actually see what they're

doing while they're inside whatever-it-is (Cosell: CuD 3:12 April 1991).

From this scenario, various questions arise, such as: do you call the Police? what would the intruders be charged with? and would your response be different if you were the owner of the resort? Someone more sympathetic to the hacker point of view illustrated the fundamentally different way in which the two groups, CSI and CU, conceptualise the ethical issues and the corresponding use of physical analogies. He responded that:

> Of course you should call the cops. Unless they are authorised to be on the property, (by the owner) they are trespassing, and in the case of picking locks, breaking and entering. However, you're trying to equate breaking into a ski resort with breaking into a computer system. The difference being: 99 times out of 100, the people breaking into a computer system only want to learn, have forgotten a password, etc. ... 99 times out of 100, the people breaking into the ski resort are out for free shit (Rob Heins CuD 3:13).

The CU accuse the CSI of preferring to use physical analogies in order to marginalise a group, rather than make use of their information for improving the security of systems:

> When you refer to hacking as 'burglary and theft' ... it becomes easy to think of these people as hardened criminals. But it's just not the case. I don't know any burglars or thieves, yet I hang out with an awful lot of hackers. It serves a definite purpose to blur the distinction, just as pro-democracy demonstrators are referred to as rioters by nervous political leaders. Those who have staked a claim in the industry fear that the hackers will reveal vulnerabilities in their systems that they would just as soon forget about (Emmanuel Goldstein: CuD 1:13).

This is one explanation of why, if physical analogies are inevitably only crude analytical approximations and rhetorical

devices with which to conceptualise computing issues, they are frequently used by the CSI in their discourse. Johnson argues in response to the claim that hackers serve a useful purpose by pointing out security faults that:

> If a policeman walks down the street testing doors to see if they are locked, that's within his 'charter'- both ethically and legally. If one is open, he is within the same 'charter' to investigate - to see if someone else is trespassing. However, it's not in his 'charter' to go inside and snoop through my personal belongings, nor to hunt for illegal materials such as firearms or drugs ... If I come home and find the policeman in my house, I can pretty well assume he's doing me a favour because he found my door unlocked. However, if a self-appointed 'neighbourhood watch' monitor decides to walk down the street checking doorknobs, he's probably overstepped his 'charter'. If he finds my door unlocked and enters the house, he's trespassing ... Life is complicated enough without self-appointed watchdogs and messiahs trying to 'make my life safe (Bob Johnson: e-mail interview).

Thus, hackers are seen to have no 'charter' which justifies their incursions into other peoples' systems, such incursions being labelled as trespass. Even comparisons to trespass, however, tend to be too limited for those wishing to identify and label hacking as an immoral act. Trespass is a civil and not a criminal offence. Onderwater, makes this distinction with his particular use of analogies: "Trespassing means in Holland if somebody leaves the door open and the guy goes in, stands in the living room, crosses his arms and doesn't do anything." In contrast, hacking involves the active overcoming of any security measures put before hackers, Onderwater sees it as more analagous to the situation whereby:

> you find somebody in your house and he is looking through your clothes in your sleeping room, and you say 'what are you doing?' and he says 'well, I was walking at the back of the garden and I saw that if I could get onto the shed of your neighbour, there was a possibility to get onto the gutter, and

could get to your bathroom window, get it open, that was a mistake from you, so I'd like to warn you ... You wouldn't see that as trespassing, you would see that as breaking and entering, which it is and I think it's the same with hacking (Onderwater: Hague interview).

(iii) Rejection of breaking and entering analogies - hackers use of physical analogies: chess vs breaking and entering

Gongrijp's description of the motives lying behind hacking was typical of the hackers I met. He concentrated on the intellectual stimulation it affords as opposed to any desire just to trespass onto computer systems . He emphasised the chess-like qualities of computer security, and was at pains to reject any analogies that might compare hacking to physical breaking and entering. Gongrijp contended that:

> Computer security is like a chess-game, and all these people that say breaking into my computer systems is like breaking into my house: bull-shit, because securing your house is a very simple thing, you just put locks on the doors and bars on the windows and then only brute force can get into your house, like smashing a window. But a computer has a hundred thousand intricate ways to get in, and it's a chess game with the people that secure a computer... it's their job to make the new release of their Unix system more secure, and it's the job of the hackers to break in (Gongrijp: Amsterdam interview).

Coggans turns the burglar analogy on its head when he argues that:

> People just can't seem to grasp the fact that a group of 20 year old kids just might know a little more than they do, and rather than make good use of us, they would rather just lock us away and keep on letting things pass them by ... you can't stop burglars from robbing you when you leave the doors open, but lock up the people who can close them for you, another burglar will just walk right in (Coggans 1990).

The implication of these combined views, is that the analogy comparing hacking with burglary fails because the real world barriers employed to deter burglars are not used in the virtual world of computing. Such preventative measures are either not used at all, or are of a qualitatively different kind to the 'doors' and 'locks' that can be used in computing. Such barriers can be overcome by technologically knowledgeable young people, without violence or physical force of any kind. The overcoming of such barriers, has a non-violent and intellectual quality that is not apparent in more conventional forms of burglary, and which therefore throws into question the whole suitability of such analogies.

(iv) Problems of using physical analogies as explanatory tools

The following excerpt is a newspaper editorial response to the acquittal of Paul Bedworth case. It compares computer addiction to a physical addiction for drugs:

> This must surely be a perverse verdict ... Far from being unusual in staying up half the night, Mr Bedworth was just doing what his fellows have done for years. Scores of universities and private companies could each produce a dozen software nerds as dedicated as he ... Few juries in drug cases look so indulgently on the mixture of youth and addiction (Ind 18.3.93: editorial p. 25).

This editorial emphasises how such analogies are utilised in an attempt to formulate ethical responses to an activity of ambiguous ethical content. As Goldstein pointed out, it becomes easier to attribute malign intent, if using such analogies succeeds in making a convincing comparison between hacking and an activity the public are more readily inclined to construe as a malicious activity. The adaptability of this technique is shown by the way the editorial continues to utilise a physical analogy in order to elicit critical responses, this time against the victims of the previously maligned

hacker: "Leaving those passwords unchanged is like leaving the chief executive's filing cabinet un-locked. Organisations that do so can expect little public sympathy when their innermost secrets are brought into public view."

The main reason why physical analogies tend not to succeed in any attempted project of stigmatisation/'ethicalisation' of hacking events is the difficulty of convincing people that events that transpire in virtual reality are in fact comparable and equivalent to criminal acts in the physical world. We have seen for example the weaknesses of breaking and entering analogies. They flounder upon the fact that hacking intrusions do not contain the same threats of transgression of personal physical space and therefore a direct and actual physical threat to an individual. With the complete absence of such a threat, hacking activity will primarily remain viewed as an intellectual exercise and show of bravado rather than a criminal act, even if, on occasion, direct physical harm may be an indirect result of the technical interference caused by hacking.

Thus the use of analogies is fraught with problems of equivalence. Whilst they may be useful as a rough comparison between the real and virtual worlds, the innate but sometimes subtle, practical and ethical differences between the two worlds mean that analogies cannot be relied upon as a complete explanatory tool in seeking to understand the practical and ethical implications of computing:

> They simply don't map well and can create models which are subtly and profoundly misleading. For example, when we think of theft in the physical world, we are thinking of an act in which I might achieve possession of an object only by removing it from yours. If I steal your horse, you can't ride. With information, I can copy your software or data and leave the copy in your possession entirely unaltered (Barlow: e-mail interview).

Information processed by computers is such that previous concepts of scarcity break down when correspondence is sought

between the real and virtual worlds. It is not just conceptions of scarcity that are affected, however, the extent to which information correlates with the real world is questionable at the most fundamental levels:

> Physical (and biological) analogies often are misleading as they appeal to an understanding from an area in which different laws hold. Informatics has often mislead naive people by choosing terms such as 'intelligent' or 'virus' though IT systems may not be compared to the human brain ... Many users (and even 'experts') think of a password as a 'key' despite the fact that you can easily 'guess' the password while it is difficult to do the equivalent for a key (Brunnstein: e-mail interview).

Physical analogies are inevitably flawed in the respect that they can only ever be used as an approximation of what occurs in 'cyberspace' in order to relate it to the everyday physical world. Thus they attempt to evaluate and understand computing activities using a more natural and comfortable frame of reference. Hence the language is often used by the CSI to describe computer attacks, and a security breach of the academic network with the acronym JANET, was referred to as the 'rape of JANET'. Spafford admitted to having one of his systems hacked into at least three times, he argued that he: "didn't learn anything in particular that I didn't know before. I felt quite **violated** by the whole thing, and did not view anything positive from it."(Spafford US interview [Emphasis mine]). The CU stresses the differences between the virtual and real worlds and contends that the use of physical language in such a situation is not warranted. For example, despite such use of the language of physicality, it is difficult to conceive of a computer intrusion that could be as traumatising as the actual bodily violation of a rape. A second, diametrically opposed, reason for questioning the validity of physical analogies would be that instead of overstating situations within computing, analogies used to describe a computer intrusion actually understate the harm caused by the intrusion due to the generic aspects of hacking identified earlier.

In John Perry Barlow's "Crime and Puzzlement" recourse is made to the metaphors comparing hackers with cowboys from the nineteenth century USA. This specific comparison of hackers with cowboys illustrates some of the problems associated with the use of metaphors. The basis of this metaphor rests upon the view of hackers as pioneers in the new field of computing, just as cowboys were portrayed as pioneers of the 'Wild West'. Such a metaphor, in addition to the above discussion of the applicability of the concepts of trespass and theft to the world of computing, provides a useful example of both the suitability and limitations of analogies in discussions of hacking. Commentators tend to 'customise' common metaphors used in the computer security debate, in order to derive from the metaphor the particular emphasis desired to further the point being argued:

> Much of what we 'know' about cowboys is a mixture of myth, unsubstantiated glorification of 'independent he-men', Hollywood creations, and story elements that contain many racist and sexist perspectives. I doubt that cracker/hackers are either like the mythic cowboy or the 'true' cowboy ... I think we should move away from the easy-but-inadequate analogy of the cowboy to other, more experienced-based discussions (Sherizen: e-mail interview).

The tendency to use the 'easy-but-inadequate analogy' applies significantly to the orginator of the cowboy metaphor himself. Thus, when I asked John Perry Barlow his views as to the accuracy of the metaphor, he replied: "Given that I was the first person to use that metaphor, you're probably asking the wrong guy. Or maybe not, inasmuch as I'm now more inclined to view crackers as aboriginal natives rather than cowboys. Certainly, they have an Indian view of property" (Barlow: e-mail interview).

More negative responses to the comparison of hackers with cowboys came from the hackers themselves:

> WHO is the electronic cowboy ... the electronic farmer, the electronic saloon keeper? ... I am not sold. I offer no

alternative, either. I wait for hacking to evolve its own culture, its own stereotypes. There was a T.V. show long ago, 'Have Gun Will Travel' about a gunslinger called 'Palladin'. The knightly metaphor ... but not one that was widely accepted. Cowboys acted like cowboys, not knights, or Greeks, or cavemen. Hackers are hackers not cowboys (Marotta: e-mail interview).

6.7 THE PROJECT OF PROFESSIONALISATION

6.7.1 Creation of the computer security market and professional ethos

The creation of the 'them and us' situation forms part of the process whereby a professional status opposed to the hacking culture and ethic is established. Examples have already been seen of the lack of cooperation that exists between the CSI and the CU in Chapter 5, it gave various reasons for the CSI not being able to trust hackers sufficiently enough for cooperation to be feasible. The antagonism that exists between the CSI and the CU contributes to a process of boundary formation, but there is also the widely-held belief that, along with legitimate reasons for differentiation between the two groups, there is also an element of manufactured difference. Below are two examples, one from the commercial sector, and one from the CU, of people who believe parts of the CSI are involved in creating a market niche for themselves from which it then becomes necessary to exclude hackers:

> Computer security industry' sounds like some high-priced consultants to me. Most of what they do could be summarised in a two-page leaflet - and its common sense anyway. A consultant - particularly in the U.S. - spends 3/4ths of his or her effort justifying the fee (Barrie Bates: e-mail interview).

> These virus programs are about to make me sick! In two years of heavily downloading from BBSs, I've yet to catch a virus

> from one. Peter Norton should be drug to a field and shot! McAffe too (Eric Hunt: e-mail interview).

The veracity of opinions such as those above may be difficult to separate from their origin in the antagonism that exists between the CSI and the CU, but allegations that 'viral hype' has been used as a means of helping to create a computer security market come from security practitioners themselves:

> It's very hard getting facts on this because the media hype is used as a trigger by people who are trying to sell anti-virus devices, programs, scanners, whatever. This is put about very largely by companies who are interested in the market and they try to stimulate the market by putting the fear of God into people in order to sell their products, but selling them on the back of fear rather than constructive benefits, because most of the products in the industry are sold on constructive benefits. You always sell the benefit first, this is selling it on the back of fear which is rather different, "you'd better use our products or else" (Taylor: Knutsford interview).

The whole process of enforcing and furthering the proprietary attitude to information outlined in Chapter 3 is further strengthened by a new language of physicality resulting from the advent of computer viruses[10]. Software is infected, and systems are spoken of in terms of being repeatedly 'raped'. Computer viruses are described in terms similar to those employed in discussions of the dangers of promiscuous sex. Prophylactic safety measures are seen to be necessary to protect the moral majority from 'unprotected contact' with the degeneracy of a minority group. Ross argues that 'viral hysteria' has been deliberately used by the software industry to increase its market sales:

---

[10] c.f Woolgar 1990.

> software vendors are now profiting from the new public distrust of program copies ... the effects of the viruses have been to profitably clamp down on copyright delinquency, and to generate the need for entirely new industrial production of viral suppressors to contain the fallout. In this respect it is hard to see how viruses could hardly, in the long run, have benefited industry producers more (Ross 1990: 80).

In addition to the practical benefits the CSI has derived from the concerns associated with viruses, the threat they pose to systems' security has been used to reinforce ideological opposition to hackers and their anti-proprietary attitudes:

> Virus-conscious fear and loathing have clearly fed into the paranoid climate of privatization that increasingly defines social identities in the new post-Fordist order. The result -- a psycho-social closing of the ranks around fortified private spheres -- runs directly counter to the ethic that we might think of as residing at the architectural heart of information technology. In its basic assembly structure, information technology is a technology is a technology of processing, copying, replication, and simulation, and therefore does not recognise the concept of private information property (Ross 1990: 80).

The boundary formation exercise necessitates the exclusion of hackers from influence within computing, whilst, at the same time, developing a consistent ethical value system for 'legitimate' security professionals. An example of boundary formation in action is the advent of computer viruses and worms and the particular case of Robert Morris and the Internet Worm. Cornell University published an official report into the Internet Worm incident, concluding that one of the causes of the act was Morris' lack of ethical awareness. The report censures the ambivalent ethical atmosphere of Harvard, Morris' alma mater, where he failed to develop in a computing context a clear ethical sense of right and wrong. Most significantly, the judgement made upon the Morris case was full of implicit assumptions that betrayed a boundary forming process in the way it

stressed the need for professional ethics in opposition to those of hackers.

Dougan and Gieryn (1988), sum up the boundary-forming aspects of responses to the Internet Worm in their analysis of the e-mail debate that occurred shortly after the incident. The computer community is characterised as falling into two schools of thought with regard to their response to the event. The first group is described as being organised around a principle of 'mechanic solidarity, the second, one of 'organic solidarity'. The mechanic solidarity group's binding principle is the emphasis they place upon the ethical aspect of the Morris case, his actions are seen as unequivocally wrong and the lesson to be learnt in order to prevent future possible incidents is that a professional code of ethics needs to be promulgated. These viewpoints have been illustrated in this study's depiction of the hawkish response to hacking. The second group advocates a policy more consistent with the dovish element of the CSI and those hackers that argue their expertise could be more effectively utilised. They criticise the first group for failing to prevent 'an accident waiting to happen' and expecting that the teaching of computing ethics will solve what they perceive as an essentially technical problem. The likelihood of eliminating the problem with the propagation of a suitable code of professional ethics seems to them remote:

> I would like to remind everyone that the real bad guys do not share our ethics and are thus not bound by them. We should make it as difficult as possible -- (while preserving an environment conducive to research) for this to happen again. The worm opened some eyes. Let's not close them again by saying 'Gentlemen don't release worms' (Dougan and Gieryn 1988: 12).

The hacker Craig Neidorf known as 'Knight Lightning', in his report on a CSI conference, underlines the theory that the debate over hacking centres upon a project of professionalisation, with the

argument that what mostly distinguishes the two groups is the form, rather than content of the knowledge they seek to utilise:

> Zenner and Denning[11] alike discussed the nature of Phrack's[12] articles. They found that the articles appearing in Phrack contained the same types of material found publicly in other computer and security magazines, but with one significant difference. The tone of the articles. An article named 'How to Hack Unix' in Phrack usually contained very similar information to an article you might see in Communications of the ACM only to be named 'Securing Unix Systems'. (Craig Neidorf: CuD 2.07).

The implication is that hackers' security knowledge is not sought due to reasons other than its lack of technical value; instead the CSI fails to utilise such knowledge more fully because it interferes with their boundary-forming project that centres upon attempting to define the difference between a hacker and a 'computer professional':

> Ironically, these hackers are perhaps driven by the same need to explore, to test technical limits that motivates computer professionals; they decompose problems, develop an understanding of them and then overcome them. But apparently not all hackers recognise the difference between penetrating the technical secrets of their own computer and penetrating a network of computers that belong to others. And therein lies a key distinction between a computer professional and someone who knows a lot about computers. (Edward Parrish 1989).

Another interesting example of the similar traits that the CSI and CU share in common, is the case of Clifford Stoll's investigation of an intrusion into the Berkeley University computer laboratories,

---

[11] The former was the defence lawyer for Craig Neidorf in the E911 trial of 1990, Dorothy Denning being a computer scientist from Georgetown University, Washington, with an academic interest in CU issues.

[12] CU electronic magazine

which he subsequently wrote up in the form of a best-selling book, The Cuckoo's Egg. Thomas points out that:

> Any computer undergrounder can identify with and appreciate Stoll's obsession and patience in attempting to trace the hacker through a maze of international gateways and computer systems. But, Stoll apparently misses the obvious affinity he has with those he condemns. He simply dismisses hackers as 'monsters' and displays virtually no recognition of the similarities between his own activity and those of the computer underground. This is what makes Stoll's work so dangerous: His work is an unreflective exercise in self-promotion, a tome that divides the sacred world of technocrats from the profane activities of those who would challenge it; Stoll stigmatises without understanding (Thomas 1990).

What makes Stoll's behaviour even less understandable is that throughout the book he recounts how he himself engages in the same kind of activities that he criticises others for indulging in. This fact that Stoll labels hackers as 'monsters' despite the fact he shares some of their qualities[13] is indicative of the boundary forming process the CSI have entered upon. The process also involves other groups that are involved in the de facto marginalisation of hackers whilst not actually being directly involved in computing, examples of such groups are the various government agencies and politicians involved in the drafting of legislation about hacking. Combined together, these groups have contributed towards a response to hacking that has been labelled a 'witch-hunt' mentality by some observers.

6.7.2 Witch-hunts and hackers

Part of the cause of the witch-hunt mentality, that has allegedly been applied to hackers, is the increasing tendency within society towards the privatisation of consumption examined in the

---

[13] Thomas' review of The Cuckoo's Egg includes numerous examples of Stoll indulging in such activities as borrowng other peoples' computers without permission and monitoring other peoples' electronic communications without authorisation.

early chapters. The pressures to commodify information can be seen as an extension of the decline of the public ethos in modern society which is accompanied by the search for scapegoats that will justify the retreat from communitarian spirit. The hacker is the latest such scapegoat of modern times in a series including Communism, terrorism, child abductors and AIDS:

> More and more of our neighbours live in armed compounds. Alarms blare continuously. Potentially happy people give their lives over to the corporate state as though the world were so dangerous outside its veil of collective immunity that they have no choice ... The perfect bogeyman for modern times is the Cyberpunk! He is so smart he makes you feel even more stupid than you usually do. He knows this complex country in which you're perpetually lost. He understands the value of things you can't conceptualize long enough to cash in on. He is the one-eyed man in the Country of the Blind (Barlow 1990: 56).

This is the root of peoples' fear of hackers and the reason why they are labelled as deviant within society despite the fact that, as we have seen above, hackers share some of the same characteristics as their CSI counterparts. The simultaneous existence of shared characteristics and deviant status for hackers is a necessary result of the fact that:

> The kinds of practices labelled deviant correspond to those values on which the community places its highest premium. Materialist cultures are beset by theft (although that crime is meaningless in a utopian commune where all property is shared) ... The correspondence between kind of deviance and a community's salient values is no accident ... deviants and conformists both are shaped by the same cultural pressures -- and thus share some, if not all, common values -- though they may vary in their opportunities to pursue valued ends via legitimate means. Deviance ... emerges exactly where it is most feared, in part because every community encourages some of its members to become Darth Vader, taking 'the force' over to the 'dark side' (Dougan and Gieryn 1990: 4).

The vocalised antagonism between the CSI and CU and the exaggerated portrayals of the media examined in this chapter are part of the process whereby hackers are marginalised and defined as deviant. In the quotation below Stoll is singled out to personify this process but the method he uses is held in common with all the other figures quoted in this chapter who contribute to the 'them and us' scenario by the strength of the views they express and the analogies they choose to express them with:

> Witch hunts begin when the targets are labelled as 'other', as something quite different from normal people. In Stoll's view, hackers, like witches, are creatures not quite like the rest of us, and his repetitious use of such pejorative terms as 'rats,' 'monsters,' 'vandals,' and 'bastard' transforms the hacker into something less than human ... In a classic example of a degradation ritual, Stoll -- through assertion and hyperbole rather than reasoned argument -- has redefined the moral status of hackers into something menacing (Thomas 1990).

6.7.3 Closure - the evolution of attitudes

The witch hunt process is a device to facilitate what Bijker and Law (1992) have analysed as closure. The notion is usefully illustrated by examining the evolution of society's attitudes from the benign tolerance of the early MIT hackers to the present climate of anti-hacking legislation. In addition to Levy's identification of three generations of hackers[14], Landreth suggests the arrival of a fourth generation of hackers when he talks of a major change occurring in the CU around about the time the elitist hacking group he joined known as the "Inner Circle" was set up. In addition to the effect of the increased dispersal of micro-computers, there was also the effect of the hacker movie *Wargames*.: "In a matter of months the number of self-proclaimed hackers tripled, then quadrupled. You couldn't get through to any of the old bulletin boards any more - the telephone

[14] c.f. Appendix 2 for a full account.

numbers were busy all night long. Even worse, you could delicately work to gain entrance to a system, only to find dozens of novices blithely tromping around the files" (Landreth 1985 :18). These 'wannabe' hackers reflect the relative immaturity and absence of the original hacker ethic that characterises the latest manifestation of hacking. Chris Coggans from the Legion of Doom concurs with this identification of a change in the basic nature of the CU environment. In the early days:

> People were friendly, computer users were very social. Information was handed down freely, there was a true feeling of brotherhood in the underground. As the years went on people became more and more anti-social. As it became more and more difficult to blue-box the social feeling of the underground began to vanish. People began to hoard information and turn people in for revenge. The underground today is not fun. It is very power hungry, almost feral in its actions. People are grouped off: you like me or you like him, you cannot like both ... The subculture I grew up with , learned in, and contributed to, has decayed into something gross and twisted that I shamefully admit connection with. Everything changes and everything dies, and I am certain that within ten years there will be no such thing as a computer underground. I'm glad I saw it in its prime (Coggans: e-mail interview).

Thus one reason for the changing nature of the computer underground is simply the fact that more would-be hackers arrived. 'Elite' hackers such as Coggans felt that this cheapened in some way the ethos and atmosphere of camaradarie that had previously existed within the CU. Feelings of superiority which help to fuel the motivation of a hacker had become undermined by the advent of too many 'wanna-be' young hackers. Sheer numbers alone would mean the demise of the previous emphasis hackers placed upon sharing knowledge and the importance of educating young hackers. The idiosyncratic actions of the first generation hackers, within the isolated academic context of MIT, were often praised for their inventiveness. Similar actions in the wider modern computing

community tend to be automatically more disruptive and liable to censure.

The reasons for this change in attitude are inextricably linked with the evolution of computing as a technology. Herschberg argues that computer security can be compared to the experiments of the Wright brothers, yet apart from such peripheral 'dovish' sentiments, the climate within the CSI and society as a whole is increasingly unsympathetic to the claims by hackers that they represent innocent intellectual explorers: closure in computer security has occurred. Leichter's perception of the evolution of hacking is at odds with that of Herschberg. He too uses an airplane analogy but prefers to emphasise that:

> When the first 'airplane hackers' began working on their devices, they were free to do essentially as they pleased. If they crashed and killed themselves well, that was too bad. If their planes worked - so much the better. After it became possible to build working airplanes , there followed a period in which anyone could build one and fly where he liked. But in the long run that became untenable ... If you want to fly today, you must get a license. You must work within a whole set of regulations (Jerry Leichter: CuD 4.18).

Over time, technologies develop, and as a result, people's interactions with that technology, even if they remain unchanged, will be viewed differently as society adapts to the changing technology. An example of this is the changing role of system crashes. In the earliest days of computing, the computers functioned by means of large glass valves, which after relatively short periods of use were liable to over-heat, thus causing a system crash. Even if hackers were responsible for some of the system crashes that occurred, the fact that they were equally liable to be caused by other non-hacker means, led to a climate whereby hacker-induced crashes were accepted as a minor inconvenience even when they were extremely disruptive by today's standards. This is an example, therefore, of the importance of taking into account the societal

context of an act involving technology before an evaluation of its ethical content is made.

6.8 CONCLUSION

This chapter has traced the origin of the ethical debate between the CSI and the CU, showing how the novel nature of some of the situations thrown up by computing has resulted in a process of negotiation. This process takes the form of markedly different ethical responses to the novel situations being made and competing with each other. The contrasting interests and perspectives of the two groups is highlighted by the fact that whilst hackers see their activity as manifesting ethical concern over potential governmental and commercial abuses of privacy, the CSI prefers to see the activity as unethical or as evidence of a general decline in social values.

There are two important elements of doubt regarding the view of the CSI. Firstly, the argument that hacking is intrinsically unethical is weakened by the fact that, as Levy documents, the same acts of hacking that are now criticised as immoral, were benignly tolerated in the days of the early MIT hackers. Bloombecker even goes so far as to claim that what would nowadays be labelled a computer criminal, helped to make computing what it is. Cohen also asserts, that unofficially, hackers are often used commercially to check the security of systems. Secondly, the chapter has shown, that an increasing aspect of computing is the way in which it produces novel situations where there seem to be no clear-cut boundaries between right and wrong. This is most noticeable in the situations produced by technology that are most divorced from everyday experience, typified by the notion of cyberspace. Ethical uncertainty concerning hacking is also exacerbated by the fact that the activity is often motivated by a series of complex factors. The fact that there is a keen debate, both within the CSI, and between the CSI and the CU, implies that any purported immorality of hacking is due to the social shaping of a perception that has evolved from the MIT days of benign tolerance to the present atmosphere of criminalisation.

An important part of this process of social shaping is the way in which physical analogies are used in the formation of computer ethics. They are being increasingly used in professional discussions of the issues as part of the process of group delineation. Where previously there were only blurred or indefinite computer ethics, physical analogies are now used to establish clearer computing mores. The need to use physical analogies in the first place arises because hacking takes place in the qualitatively new realm of human experience: cyberspace. The fact that the real world and cyberspace are such different realms has led to a need to explain and make ethical judgements about hacking from a conventional frame of reference, that is, using analogies based upon the physical world.

The constant use of physical analogies and metaphors in discussing the legal and ethical issues of hacking is thus an attempt to redefine, in a practical manner, the concept of informational property rights, as they are to be applied in the computer age. The use of analogies is much more common within the CSI than it is from hackers themselves. This is because the CSI have a general need to make comparisons between cyberspace and the real world in order to legitimate their role and to demonise the CU. Hackers do not have this need; their behaviour is based upon accepting computing as a realm of intellectual and social experimentation, and they find it attractive because of the very fact that it is different from the real world.

In summary, there are perennial claims from each successive generation that the youth of the age are largely unethical, and that they are harbingers of a break-down in the general moral order. Such claims are perhaps an inevitable part of the human condition, and its inter-generational relations. This study, however, is more concerned with the specific aspects of computing that give rise to qualitatively new circumstances facing computer users, the ethics of which are indeterminate. These situations encourage behaviour, which, to be recognised as unethical, assumes that an adequate and convincing comparison can be made with non-computing situations. It is the difficulty of attempting to conceptualise the ethics of

computer-induced scenarios that leads to attempts to translate them into a more easily understood and common-place experience.

The chapter shows, however, that there is doubts as to whether 'real-world' ethics can be transposed in such a literal manner. This is illustrated by the various examples given of the CSI's alleged double standards. These examples imply that the vagueness of computing ethics is such that any professional code of ethics that is produced is likely to be more the result of one group enforcing its value system on another group, rather than one group having any inherently superior moral advantage in the ethical debate.

The process whereby one group's value system can be imposed upon another has been analysed in a frame of reference that compares the increasing marginalisation of hackers from mainstream computer usage to the practice of witch-hunts. One analysis of the gradual stigmatisation of hackers is that they have been part of a degradation ritual whereby a more dominant social group has progressively alienated them from 'normal' society in order to promote its professional interest. The role of the media in this process has been shown by the way it projects hackers as stigmatised 'others', thus aiding the boundary forming professionalisation process of the CSI.

Particular examples of the process of group differentiation and professionalisation have been given, relating to the advent of viruses and the specific case of the Internet Worm. The likelihood of eliminating threats to computer security with the propagation of a suitable code of professional ethics seems remote considering the extent of the CU's ethical disagreement with the CSI and the thrill obtained from the very fact that the CU is 'underground'. Despite this, once the process of professionalisation has been initiated, the temptation is to proceed to codify the nascent but dominant group's response to computing's ethical dilemmas, by means of legislation.

The subsequent closure of computing technology has occurred to such an extent that the hippy-like ethos of the CU looks increasingly anachronistic in the 1980's and 90's. In so far as hackers have represented a force of anti-capitalistic information-

sharing, their stance seems to have absorbed within the state's sponsorship of the development of computing technology. The second generation hard-ware hackers such as Steve Wozniak, have seen their 'wholesome and green' product (hence the name 'Apple') brought to the masses as indeed they wished, but significantly as a commodified product. This is perhaps a reflection of the market's ability to co-opt and absorb radical change. It threatens, in the case of hackers, to undermine their status as a group embodying alternative values. The new generation of 'wanna-be' hackers, is significant because it represents more than simply adolescent boys intrigued by the intellectual challenge and feelings of power of illicit computing. In addition, they also represent the increasing tendency of information to be viewed as a tradeable commodity in the form of 'Amiga kid'-type groups. Their illicit blackmarket activities and their seemingly amoral views regarding the ethical implications of accessing and manipulating other peoples' information represents the extreme end of a spectrum which also includes the activity of 'benign' hackers. It is a spectrum whose various points reflect some of the ethical issues that society still has to satisfactorily address regarding information and the implications of its changing properties.

An example of the unsettled nature of society's response to information is the doubt that still remains regarding the effects of its policy of closure towards hackers. The question still arises from the above analysis of whether the evolution of attitudes towards the CU is in response to a change in its nature towards a more crime-orientated environment, or whether the increased tendency to perceive and portray hacking as a criminal and unethical activity has taken on the quality of a self-fulfilling prophecy, driving would-be 'pleasure hackers' into the arms of the criminal underground. The implications of this latter scenario are examined in the next chapter.

Chapter 7 - Hacking and Legislation

7.1 INTRODUCTION

7.2 CLASSIFICATIONS OF COMPUTER CRIME

7.3 CRIMINAL ACTIVITIES OF HACKERS

7.4 PRESSURES TO CRIMINALISE

7.5 'SYMBOLIC LEGISLATION'

7.6 THE PARLIAMENTARY DEBATE

7.7 ISSUES IN COMPUTER MISUSE LEGISLATION

7.8 PROBLEMS OF ENFORCEMENT

7.9 LEGISLATION AND THE EVOLUTION OF HACKING: MIT TO ALACATRAZ

7.10 CONCLUSION

7.1 INTRODUCTION

Society's attempts to reconcile competing views about informational property rights are reflected in the debate as to whether non-malicious system cracking/browsing should be treated as a criminal act. Anti-hacking legislation is the logical extension of the stigmatisation process identified in the previous chapter. Moral language is used in both legislative debates and in the law enforcement techniques adopted, exacerbating the 'them and us' feelings of polarisation. This chapter explores the specific case of the 1990 United Kingdom Computer Misuse Act. Material is thus taken from the parliamentary debates and committee readings of the Act, which was brought to the House of Commons as a Private Member's Bill, by Michael Colvin MP. This was after a previous attempt by Emma Nicholson to pass a similar bill had been thwarted through a lack of parliamentary time. The resort to legislation raises a number of issues to be addressed in this chapter, as highlighted in the following quotation:

> Through legislation we can turn what the hackers do into a crime and there just might be a slim chance that we can stop them. But that won't fix poorly designed systems whose very existence is a violation of our privacy (Goldstein 1993).

Firstly, legislation is far from certain to eliminate hacking, and may indeed best be described as largely symbolic. Secondly, it reiterates a common theme running throughout this study, namely the security weaknesses of many systems and the recurrent failure to deal with them; a failure that is unlikely to be remedied with the application of legislation. In addition, there is a third issue, namely, the potential problem associated with even successfully implemented legislation: the danger of driving hacking knowledge into the hands of the criminal fraternity.

The chapter illustrates some of the difficulties faced by legislators in responding to the pressures to criminalise hacking, and

in attempting to draft laws that will adequately cover some of the new situations thrown up by computing technology. Daniel Cunliffe, an Edinburgh University researcher, points out that:

> I think the concepts of theft and trespass do need to be applied in order to define computer crime. However, it is obvious that they will require legal redefinition if they are ever to be acted upon. Theft and trespass work well at an intuitive level but the real (virtual?) world of computer systems is too complicated to allow a simple application of existing laws. It requires very careful drafting by people that know the law and people who understand the nature of computers. Even then, there are likely to be problems with proof, e.g. how do I prove that someone broke into my system and sent off obscene mail to my ex-wife in my name? The whole area presents a very interesting challenge to the legal profession and to the way people think about computers (Cunliffe: e-mail interview).

The challenge to the legal profession and the rest of society, resides in the fact that, as we have seen in chapter 3, information has an ambivalent status as a commodity and is something to which property rights cannot easily be assigned:

> I think it stems from the cultural (in a sociological sense) basis which we use to attach financial values to things. Cars and houses have a financial and personal value which most people can negotiate and agree on. If we suffer loss or damage to this kind of object we can usually gauge that loss and society can work out some recompense for that loss (insurance, punishing offenders etc.) I think information, especially electronic information is different. We don't have the necessary agreed mechanisms on which to establish its financial and personal value. By its very nature it is very easy to move ('steal'). Thus given the lack of effort in 'stealing' it and the lack of any perceived damage (on behalf of the thief) it is not seen (by them) as a real crime (Dr David England Glasgow University: e-mail interview).

In this context, hackers fail to perceive much of their activity as a crime. They see the new emphasis being deliberately placed

upon ethics in the professional worlds of business and science as part of an attempt to develop a coherent response to the contradictions associated with information's evolving nature: "For all the trumpeting about excesses of power and disrespect for the law of the land, the revival of ethics, in the business and science disciplines in the Ivy League and on Capitol Hill ... is little more than a weak liberal response to working flaws or adaptational lapses in the social logic of technocracy" (Ross, 22: 1990). The 'weak liberal response' has taken the form of legislation to outlaw hacking activity:

> Lobbying by computer users for the criminalisation of cruelty to (their) computers has been extensive and vociferous. The imposition of criminal sanctions is seen as some sort of magic talisman ... the law takes the computer too seriously. All sorts of magical qualities are ascribed to the machine. The debates on the Computer Misuse Act are replete with demonic images of hacking and its consequences. The computer is the ultimate bogeyman and has produced a knee jerk reaction from Parliament (Ian Lloyd- Strathcylde University Law Department, 9. 6.1993: Edinburgh Univ AI Dept. Seminar).

Chapter 5's statistics and their illustration of the relatively low threat posed by hackers give credence to the view that the legislative targeting of hackers is a misapplication of resources. This chapter explores Lloyd and Cunliffe's assertions that there has been an over-reaction to the problem of hacking, and that attempts have been made to apply unsuitable notions of property rights to the realm of computing.

Various examples are given in this chapter of pressures, from numerous sources, to criminalise hacking. The soubriquet of 'symbolic legislation'[1] is then introduced to examine the view that laws are being passed against hacking for their symbolic qualities rather than any hope of efficacy: the Computer Misuse Act is evaluated with particular reference to its professed objectives of deterrence. Three of the main factors that are likely to limit the

[1] A phrase first used in relation to computer misuse legislation by Hollinger and Lanza-Kaduce (1988).

efficacy of legislation designed to prevent hacking are also examined. The first of these is the problem law-makers encounter when trying to take into account the intent of the hacker; the intrinsically anonymous nature of computer communication makes gauging intent extremely difficult. Secondly, it is found that many conventional legal concepts fail to transpose literally into the world of cyberspace, for example, when computer intrusion is compared to 'breaking and entering', the comparison begs the question of what is actually 'broken'. Thirdly, legislators have difficulties basing policy upon a dearth of reliable statistics. In the context of this 'information gap' there seems to be a tendency for spurious computer crime estimates to gain legitimacy if for no other reason than they are repeated often enough.

Given the above problems, and assuming that effective legislation results in the imprisonment of hackers, the chapter concludes by raising questions as to the likely implications of the risks of pushing hacking techniques into the reach of the conventional criminal underground.

7.2 CLASSIFICATIONS OF COMPUTER CRIME

Hollinger and Lanza-Kaduce (1988) identify four categories of computer crime.

1. The computer is the specific 'object' of a direct act. This refers to destructive acts aimed specifically at the hardware of the computer itself. One dramatic example is the Californian Highway Patrolman who shot the computer terminal he was using with his magnum[2].

2. The 'symbolic' use of the computer and its output to defraud. The example the authors give is that of the 'false invoice scam'.

3. The computer as the 'instrument' of the offence. In these incidents computing equipment is used to carry out theft or

[2] c.f. Bequai 1987

trespassing acts which could only have previously been carried out by physically stealing from a person or their property.

4. The computer as the 'subject' of the offence. In this category, the computer and the information it contains is the focus of the activity. The implication is that a breach of security or confidentiality is being carried out for its own sake and not for any pecuniary gain.

This chapter will deal mainly with the distinction to be made between categories 3 and 4. The former, it will be argued, is the continuation of traditional forms of fraud and industrial espionage, whereas the latter forms a qualitatively new activity only made possible by the technological advances of computing. It is the fundamental change in the nature of information due to computing technology, examined in chapter one, that forms the basis of category 4 and gives rise to the issues analysed in this chapter as to whether traditional notions of criminality can be effectively applied in certain computing situations.

7.3 CRIMINAL ACTIVITIES OF HACKERS

As would be expected, most of the emphasis placed upon criminal types of motivation for hacking comes from the CSI. The criminal element of hacking was, however, recognised by several of the hackers I spoke to, one of whom, Mike, whilst claiming it was only to see whether it could be done, demonstrated on the table of the cafe in which the interview took place, his prototype magnetic credit-card copier:

> By the way, this is the card-copier, I'm proud of it. [So what does it copy?] Everything. [Everything with a magnetic strip?] Yeah, I'll let you hear how a credit-card sounds, the trick is you take two cards, you slide them through here at the same time, yeah well it gives the same sound but then it copies from this one to this one, you can also use this for credit cards, there's a different sound, I can hear what kind of card it is through the ear-phones (Mike: Utrecht interview).

Whilst interviewing at the headquarters of Hack-Tic in Amsterdam, I was also shown their latest prototype touch-tone dialler which they were in the process of miniaturising further, and which is used as a means of phreaking free phone calls by emulating electronically the switching tones of the international digital phone systems:

> Well, I can show you something, this device, this chip, is also available in a very small package, it will fit into this whole thing [a small touch-tone dialler case he bought from the Dutch equivalent of Argos, on my arrival]. This whole prototype will be in here [large sandwich board of electronics], he [a colleague] is working on the board now. What this basically does is, it's a touch-tone dialler that has extra features which mean you can make tones which are called C5 to control the phone system and to tell phone switches in other countries that they should complete calls without charging you for it, so with this system you can make free phone calls, and its all going to be in a little dialler this big, it's pretty nifty ... you can have it make these tones and try things at different times, there's all these protocols for in-band telephone signalling in there, it's fully programmable ... We make our phone-calls with this type of technology so it doesn't cost anything (Gongrijp: Amsterdam interview).

Whereas Gongrijp and his colleagues were not, or would not admit to being, interested in the potential commercial aspects of their activity, Mike, another Dutch hacker, was much more forthcoming. When I asked him about monetary reward being a possible motivating factor behind hacking, he related how:

> A friend of my brother ... is only concerned with the money he gets for it, [and] all kinds of schemes he has to make things. Free phone calls, there's a lot of business in it. They sell cards, copy cards and things like that. Car phones: they change the chip with the ID of the car phone, things like that (Mike: Utrecht interview).

He then proceeded to give more details of his own personal

involvement in a scheme aimed at funding an excessively large phone-bill that had been accumulated as a product of his hacking exploits:

> The first system we attacked was the Spanish Telephone system, it was about seven years ago, we didn't have a meter to check the costs, later we found that when we called Spain, there was one special tone which activated the computer and we had a phone-bill of 10,000 guilders, so we made little boxes, blue boxes, and me and my brother went to Spain with the boxes. Well, we first sent the taxi-driver to pick up the boxes and then waited to see if the taxi-driver came back without the police and then we took the boxes and sold them to all kinds of people, dealers of cars and such like, it was very hard to deal with the Spanish people because they can't get money from the banks very easily, they have to show where the money is going, per box we asked 1,500 guilders, so after 10 boxes we paid the bill and got back to Holland (Mike: Utrecht interview).

Mike believes that there is the possibility that hacking expertise will become more widely used by criminal elements in society:

> If you keep it illegal then I think in the future there will be more people who will be interested in it, really malicious people, right now there aren't so many people who want to sell it to espionage or companies or whatever, but I think in the future there will be more people, you always see people who are interested but they don't have the means to hack themselves. There was a hackers' party, the 'Galactic hackers' Party' in Amsterdam and we were trying to make free phone calls and always someone behind you, some foreigner from Egypt "free phone calls, free phone calls". The only thing he could say in Dutch was "free phone calls", and they offer a lot of money to make free phone calls and stuff: often companies if they want to know something else about other companies - like a friend of mine had an account that would check out all companies, they were offered money to check out other companies but when they wouldn't do it, they would get in trouble (Mike: Utrecht interview).

For obvious reasons, it was difficult to look in any depth at hacking conducted solely for criminal or monetary purposes, or even to check the absolute validity of claims such as Mike's above. What I did see of the above instances seemed to be real methods of fraud, and the hackers I spoke with, with the exception of the Zoetermeer group, all had knowledge of each other and seemed to verify each other's claims and accounts. Hacking with criminal intent or for monetary gain of some sort, appeared, from my interviews in Holland at least, to be conducted on the fringes/margins of main-stream hacking. The pressure to commercialise their activity may, however, be increasing as techniques become more widely desired by such groups as drug dealers.

Ralph, another Dutch hacker, also gave his perspective on monetary-induced hacking. In an attempt to quantify a perhaps inevitably vague area, I asked him to give me a percentage figure for the number of hackers that hack for monetary gain, he replied:

> No, you can't say it in percentage, I'd guess it's about five persons in the whole of Holland that do it for the money. For instance I had a hack and somebody wanted to publish it, he gave me money for it. Now, did I do it for the money. No, not initially, initially I did it for the kick, not because it was illegal but for the kick. Okay, so I earned a little money with it, big deal, I didn't do it for the money, and another reason is convenience, pure convenience. It is very convenient if you can make free phone calls, it is absolutely convenient if you can pull copies off magnetic cards, it is very easy if you can get your TV at home without a de-scrambler, things like that. And it's not a kick, it's not a thrill, it's not that it's illegal, it's just pure convenience (Ralph: Utrecht interview).

One group which is much more criminal-minded, and recognised as such by Rop, Mike and Ralph, are known as the "Amiga kids", after the computers they most use. When discussing viruses Mike described how:

> There are a lot of viruses in the Amiga world. That's one of the groups they have to get rid of, the Amiga kids, that's a real

pain in the arse. Also for hackers, if we hack a system and they find out about it, like making free phone calls, they spread it. It's incredible, those guys are really destructive, because when they use something they use it for software, we use it occasionally for hacking or making calls but they use it 24 hrs a day for software, they'll do anything for software, they use and abuse credit cards and things like that. Anything for software, and a few of them, I know, are the ones that write viruses to combat other groups, to put viruses in the programs of other groups, I hate those guys. [Just like gangster warfare?] Yeah, here in Utrecht there are a lot of these groups and they card a lot of stuff, you know carding? Using credit cards to get stuff, but illegally. They wear Rolexes, little kids on the street with Rolexes around their wrists it's incredible (Mike: Utrecht interview).

The hackers that form the basis of this study were at pains to disassociate themselves from such groups, although there seems evidence to suggest potential for hacking-related activities to branch into criminal activity. Maelstrom[3], a hacker from the USA related how:

In 1989 a local friend put up a world headquarters BBS for the West German group Red Sector Inc.. They were into writing Amiga demos, and were one of the top ten groups in the world, which got us a lot of interesting and well-known callers. We obtained a voice mailbox and put up a codeline on it, which was very popular for a long time. RSI made me an offer: if I would give them stolen AT&T calling card numbers to enable them to call the USA, they give me all the hardware I needed to have the ultimate computer system. I was offered computers, high speed modems, hard drives, and software ... the only catch was their method. Using CBI or TRW's computer, some people use credit card numbers to steal merchandise, and by having stolen stuff sent to West Germany, they were able to escape detection when the theft was discovered since the post office there didn't keep records. This was against my morals, and I dropped out of the scene for a while (Maelstrom: e-mail interview).

[3] A fuller account of his activities is contained in the case-study section of Appendix 2.

7.4 PRESSURES TO CRIMINALISE

The previous chapter has illustrated this tendency to portray hackers as either criminals by nature or as in constant danger of becoming criminals. Hylton Boothroyd of the University of Warwick Business School, points to the fine dividing line between hacking and more criminal activity:

> I see the traditonal curious hacker who makes no alteration to what he looks at and uses no information to the detriment of others as practising a particular form of intellectual curiosity. However, like the adverts encouraging you to treat fire with respect, he can in an instant be tempted to transform himself into a criminal (Boothroyd: e-mail interview).

This section shows how such perceptions facilitate the criminalisation of hacking. One of the best illustrations of the differences in approaches to the question of whether hacking should be viewed as a criminal act is the marked contrast in the perceived applicability of the breaking and entering analogy. Hackers prefer to compare computer intrusion to being tempted to walk into somebody's house when the door has been left open. In the case of such negligence, and assuming that no damage is done (such an intrusion will be inevitably non-violent because of its non-physical nature), hackers argue that even if the morality of such an intrusion is questionable, there are insufficient grounds for making it a criminal offence.

> In common sense as in criminal law there exists the notion that the victim of a crime is partly or fully responsible if the crime was made possible by negligence on the victim's part ... if I don't lock my car and it is stolen, my insurance company won't reimburse me and the pepertrator of the crime will get away with a lenient sentence, as he was led into temptation by me and it is partly my fault that the car was so easy to steal ... Common sense tells most people that 'breaking' into a wide-open computer system is not a crime - if there was sensitive information in the computer, it wouldn't be wide open, would it? Sadly enough that kind of reasoning doesn't hold. Security

on many government and research facilities is appalling (Freiss: e-mail interview).

Despite the hackers' argument that breaking into a system that is wide open should not be labelled a crime, the legislation that has been passed regarding hacking treats computer intrusion more harshly than it would its physical counterpart. The 1990 Computer Misuse Act, for example, holds it as an offence to intentionally obtain unauthorised access to a program or data held on any computer, whereas the act of physical trespass, unaccompanied by any aggravating conduct, is not criminal, but rather a civil offence. Hackers argue that this discrepancy between the real and virtual worlds is being systematically used against them. There have been, for example, various instances in the US where hackers have claimed that their first and Second Amendment rights have been infringed in a manner that would not have been allowed if the situation had arisen in relation to a paper-based medium[4]. In a similar way, the application of a punitive legislative response to hacking in excess of that applicable to a physical intrusion is seen as inherently unjust. The charge from the CU is that a failure of the CSI to deal with security weaknesses has led to increased pressure to criminalise hacking, as a means of reducing the activity whilst simultaneously avoiding having to fix the faults it draws attention to. The structure of Ken Thompson[5]'s 1984 Turing Award Lecture unwittingly adds weight to this charge by the way in which it closely links the ethical, legal, and technical issues of hacking. The basis of the speech was a description of the ease with which undetectable bugs can be introduced into programs, and the subsequent implication that error-free software is easier to obtain from a trusted source. This lack of assurance about technical security leads to the search for a non-technical solution. Thompson, thus argues for a sharper legislative response to hacking:

---

[4] c.f. Sterling's (1993) coverage of the Steve Jackson's Game incident (pp 138-146).
[5] A programmer, and winner of the 1984 Turing Award.

> I would like to criticise the press in its handling of the 'hackers', the 414 gang, the Dalton, gang etc. The acts performed by these kids are vandalism at best and probably trespass and theft at worst. It is only the inadequacy of the criminal code that saves the hackers from very serious prosecution. The companies that are vulnerable to this activity, (and most large companies are very vulnerable) are pressing hard to update the criminal code (Thompson 1984: 763).

The CSI shows a marked reluctance to differentiate between 'responsible hackers' and vandals. Instead, it tends to emphasise the more malicious and destructive elements of hacking, and distinctions between malevolent and harmless browsing are played down. There are strong pressures to criminalise hacking; to seek a draconian legislative response; and to treat all hacking activities as criminal.

7.5 'SYMBOLIC LEGISLATION'

Hollinger and Lanza-Kaduce (1988), along with Michalowski and Pfulh (1990) concentrate upon the process whereby computer crime legislation is produced and then passed. The former describe how, in their view, computer crime provided a useful opportunity for legislators "'to maximise their individual media exposure without offending any major constituency' (Hollinger and Lanza-Kaduce 1988: 113), and this opportunity for positive political exposure resulted in the passage of what is sometimes termed symbolic legislation, i.e. legislation whose purpose is more ideological than instrumental." (Michalowski and Pufhl 1990: 261). Michalowski and Pfuhl conclude that computer crime legislation resulted from:

> the unexpressed understanding [of legislators] that unless computer-resident information was extended the the ideological and practical protection of the law, established relations of property and hegemonic authority relations could be deroutinised by 'information thieves' ... It was within this ideological framework that the dangers of computer crime proclaimed by computer security experts and the press *made*

sense. And in the final analysis, it was this ideological framework that made the passage of computer crime laws a low-risk, high visibility opportunity for law-makers (Michalowski and Pfuhl, 1990: 271).

Vinten's analysis of hacking legislation concludes that:

> Legislation will at least raise the profile of computer security. Enforcement will be another question ... Nobody can deny the potential and actual threat of hacking. The Law can serve as one plank in its prevention and deterrrence. Increasingly the law is giving out clear signals. It is too early to judge the impact of this ... [but] one cannot but wonder if hacking will prove as intractable as the drugs and Aids issues, and whether the legal response will be as effective as King Canute trying to beat back the waves (Vinten 1990:15).

Thus there is a perception that computer crime legislation has been used as a 'bandwagon' upon which legislators and technical experts could jump in order to further their own career-orientated goals. In support of this hypothesis is the noticeable lack of public pressure for computer crime legislation. Not only was there no apparent public pressure for legislation, there are also various qualities of computer crime that may evoke particularly tolerant, even admiring, attitudes from the public. Pfuhl (Uitenbraiuer 1991:1), for example, gives the following reasons why the public may be reluctant to censure computer criminals: computer crime is comparatively rare, people are more interested, than bothered by it; people tend to admire the daring often associated with hacking exploits; most of the victims of computer crime are faceless institutions that do not appeal strongly to peoples' sympathies; elementary precautions are often omitted in the systems that are attacked which can lead to a displacement of blame from the attacker to the victim; and finally, the game element of much computer crime such as system cracking means that it is often viewed as being outside of normal moral bounds.

7.6 THE PARLIAMENTARY DEBATE

We turn now to examine the parliamentary legislative debates. In many ways these underlined the discussion taking place in the computing industry (as detailed in the previous two chapters). For example, a justification for hacking is that it provides a useful service within computing by drawing attention to system weaknesses which would otherwise remain unfixed. We have previously seen how hackers have claimed that they are victims of blame displacement from those responsible for the security of systems that have suffered a security breach. The notion of the a priori responsibility of a computer crime victim to secure his system to the best of his ability was raised by Mr Cohen MP: "In my view, a computer system that is not properly secure can potentially cause more damage than a Rambo maniac who gets hold of guns, horrific though that is. Logic surely dictates that computer owners should be legally responsible for the security of their computers just as gun owners are responsible for their guns" (Hansard Standing Committee C 28 March 1990: 88). The subsquent parliamentary responses to this point encapsulate one of the main rationales behind the criminalisation of hacking. They express the view that, since purely technical solutions to systems weaknesses are too expensive, hacking should be prevented by the use of legislation rather than technical fixes: the view expressed is that legislation is needed to make up for the unwillingness of companies to invest sufficiently in security measures: "It could be argued that perhaps one fifth of investment in a computer software system should be allocated to security. Very few companies adopt that principle" (Nicholson Hansard 88: May 1990). Legislation is thus seen as a cost-effective measure with which to confront hacking that would otherwise prove too expensive to deal with:

> In much the same way as we lock our doors to deter burglars, it is possible to protect computers, and many people do ... However, there is no complete form of protection for computers. High levels of security can be achieved but they are horifically expensive, in terms of money, inconvenience or both. Security systems tend to slow up the computer. When

speed is the essence, that can be extremely costly. We do not expect householders to turn their homes into Fort Knox. We expect them to take sensible precautions and we add to that the support of sound laws against burglary. That is precisely my approach in the Bill (Mr Colvin MP Hansard 1139: 9 Feb 1990).

The admission that there is 'no complete form of protection for computers' reiterates some of the concerns over the general state of computer security we have previously encountered in Chapter 5. Thus Mr Hogg MP asserts that "the computer industry will welcome the Bill because it cannot build into its technology the necessary safeguards to prevent hacking or other offences. At the moment such safeguards are technically impossible and, therefore, the law must fill the gap" (Hansard 1143: 9 Feb 1990). The consensus of opinion during the parliamentary debate emphasised the fact that although hackers might possess potentially useful technical knowledge, legislation should aim at their removal so that they cannot exacerbate the security weaknesses that are acknowledged to exist:

A study of 20 European companies carried out by Coopers and Lybrand showed that 19 had inadequate standards of security which were a real threat to the economic development of those companies. The report said: 'The catastrophic effects of poor security are likely to discourage organisations from becoming any more dependent on their network systems.' That suggests that there may be a level of complexity in our society beyond which, because of safety interests, we may be frightened to go. If hacking increases our fears, there will be damage to the cohesion and organisation of our society. That is a perfectly good and sufficient justification for the Bill (Mr Arbuthnot MP Hansard: 1179 1990).

The use of the word 'fears' is significant because it draws attention to an aspect of the parliamentary pressure to criminalise hacking: the fact that legislation is used as a conduit to formally express and codify elements of the 'them and us' scenario.

Dr Taylor provided me with his model of computer security which measures cost against the security provided by that expenditure. At the lower level of the model there are basic precautions such as paper shredders, and the rotation of staff between jobs if they might be likely to collude. More complicated (and therefore expensive) technical precautions are measures to introduce more secure operating systems. Encrpyted passwords (and may even be programmed to move about the operating system ahead of any potentially curious intruder), are just one example of more sophisticated access control which protects against browsing from someone who has gained access to the password file. The basic underlying factor of all these measures is the direct linear relationship between the level of security obtained and the expense incurred. Secure, technically sophisticated, operating systems may involve man-years of effort.

Dr Taylor described his view of what role, given this cost-security scenario, legislation has to play:

> If there is no law in place to protect information, then according to the value of your information's sensitivity, you have to install appropriate technical measures which cost more and more money as they become more and more sophisticated to protect your information ... then you don't need these higher levels of sophistication, because you know that in fact as a private sector user, if anyone starts trying to get into your system and get at things like passwords and your log of events ... you prosecute. So my view of the Computer Misuse Act is that it's trying to provide a legal procedure, which will provide quite a lot of protection to quite sophisticated systems which then require less technical protection, so there's a trade-off ... legal measures cost quite a lot of money whatever level of security you want, because you have to put things like the Computer Misuse Act in place, provide the methods to prosecute the people that have breached it ... police time and so on ...What this means is that provided the legal protection is in place and working, it makes unnecessary the more complex levels of protection (Taylor: Knutsford interview).

Dr Taylor seems to recognise, however, that legislation may not be an unequivocally good thing:

> I suppose that is really going the wrong way because to get quite a good level of security by providing legal protection, you've still got to spend a lot of money ... whatever the breach of security. If it's a very simple one like pinching certain copies of paper, or it's a breach of an operating system, the cost of processing that particular breach is pretty constant, because you've got to invest in police time, in court time, and so on (Taylor: Knutsford interview).

It should also be recognised that for certain publicity-sensitive organisations such as banks, legislation may be an unfeasible solution. The adverse publicity that may result from taking a security breach case to the courts is likely to result in a marked reluctance to take recourse to legal solutions.

(i) Stigmatisation and analogies

This section analyses the specific parliamentary example of the stigmatisation process discussed in the previous chapter, and the contribution the choice of particular analogies and statistics pay to this process.

Analogies

The debate over the Computer Misuse Bill provides numerous examples of the tendency in discussions of hacking to make use of physical analogies with which to transpose real world criteria to the virtual reality of computing. The analogies used in the debate over the Bill compare hacking to burglary and acts of violence and the promulgation of this concept prepares the ground for further stigmatising statements. Nicholson illustrates the use of analogies with the following rhetorical rebuttal:

> Mr Cohen spoke of a new power to make a computer owner liable if a criminal commits an offence against his computer ... If a madman with a knife attacks another person in a street and then stabs himself, would the victim be liable for compensation for not taking reasonable care to prevent the man from stabbing himself? (Nicholson: Hansard 88:28 March 1990).

Similarly, Mr Powell MP contends that:

> Computer hacking has many parallels with burglary. Burglary takes many shapes or forms. It can be with intent ... or it can be aggravated burglary, as it appears in aggravated offences. Computer hacking remains astonishingly akin to the offence of burglary ... The hacker who says that he is performing a public service is doing exactly the same as the burglar who advances by way of mitigation the argument that he is performing a public service (Powell, Hansard 28 March 1990: 89 and Feb 9th 1990: 1147).

In contrast, Cohen responds: "Stabbing and burglary, are not relevant examples. If a person has been negligent, left his doors open and been burgled, I bet a lot of insurance companies have a get-out clause to avoid payment" (Hansard 28 Mar 1990: 89). Cohen's response questions Powell's belief that conventional criminal concepts can be successfully transposed into virtual reality. We see here how the use of analogies tends to encourage a continual redefining of the particular question at issue. Small changes in the analogy are used in order to question the suitability of the original premise the analogy sought to illustrate. Despite doubts such as those expressed by Cohen, the parliamentary debates leading up to the Bill explicitly sought to criminalise hacking and stigmatise hackers:

> We must think of hacking as a form of burglary. We must stigmatise such criminal activities for what they are. Because computer buffs use a different vocabulary and have a method of thought different from the conventional method that we all use does not alter the fact that the principles of criminal law

are just as clearly at stake (Powell, Hansard 9th Feb 1990: 1148).

Previously, the process whereby such stigmatisation is enacted has been referred to as a "degradation ritual". The following is evidence that at least to some extent, such a process has occurred in the parliamentary debate. Parliamentary stigmatisation can be seen as taking two closely-related forms. In the first, the motivations of hackers are impugned, and in the second, the dubious nature of hackers' motives are highlighted by a group-bonding process which emphasises the "them and us" scenario.

The following is an example of the first form, it is Dr Lewis Moonie MP's portrayal of the motivations of hackers:

> The motive ... is simple to understand - human greed. Although we do not condone theft, we can possibly understand the need or personal circumstances which may drive someone to commit that act. That is not the case with the kind of computer misuse that we are discussing. Very often the people involved are educated professional people and they have the werewithal to afford to carry out such behaviour ... Although we may not accept greed, we can understand it. The motive for malice is more difficult to comprehend ... There are many kinds of people involved and most, although not exclusively all, are men. Although I have never professed to have espoused the cause of Freud in my psychiatric work, I believe that a profound sexual inadequacy is often related to such behaviour (Dr Moonie, Hansard 1156: 9th Feb 1990).

The second aspect of the stigmatisation process: the construction of the 'them and us' scenario takes the form of, first, reinforcing group identity by underlining those qualities that produce the "us" and, second, contributing to perceptions of the alien nature of "them". An example of the former is the way in which Powell 'proves' the potential menace of hacking by referring to the social position of a figure calling for legislation to deal with hacking:

> Yesterday I received a letter from a constituent who is a leading official in one of the world's leading banks. He asked

me to support the Bill, and I am happy to assure him that I do so with enthusiasm ... When such an important official troubles to write to a Member of Parliament about a specific piece of legislation, knowing the background of his career I have not the slightest doubt that the menace of hacking and its consequences is widespread (Powell, Hansard 9th Feb 1990: 1147).

The difference between such a constituent and those of the culture against whom anti-hacking legislation is aimed is starkly apparent:

To show the sort of twisted culture that the Bill is trying to stamp out, I have an extract from a bulletin board ... stating: 'who's seen the news in the 'Sunday Times' ... page A5 ... about hacking ... and phreaking Mercury ... they also want restrictions on BBS's ... it's that stupid cow ... the Devon MP 'computer expert' [Nicholson] ... don't make me laff ... could be bad news tho ... maybe someone should assassinate her?' Did somebody suggest that hacking is a harmless culture? All that I can say is that it is a privilege and I am honoured to join my hon. Friend on the hackers' hit list (Colvin, Hansard Feb 9th 1990: 1137).

Once the sense of the 'us' has reinforced a sense of group identity, the process to establish unequivocally 'who we are not' begins: Colvin continues by relating how he hoped "that the debate will dispell any lingering belief that the computer hacker is some sort of Raffles of the microchip" (Hansard Feb 9th 1990:1142). Nicholson describes in detail various salacious and potentially destabilising aspects of hacking activity ranging from proliferation of pornography on bulletin boards to interest being shown by political groups such as the Greens, Anarchists and those behind the 'Electronics and Computing for Peace Newsletter'. She seeks to distance herself from "people who believe that they have a right of access to all knowledge and that everything should be out in the open - and should specifically be open to them". Nicholson proceeds to relate reported incidents of hackers who have allegedly 'tried to kill patients in hospital by accessing their drug records and altering

their prescriptions on computer' (Hansard Feb 9th 1990:1151 + 1153). Finally, Nicholson advocates legislation against hackers because:

> It is no good saying that people must increase their protection, because hackers are very clever. They will find a way around every form of protection that one buys or creates. That is what they are there for. They make a great deal of money out of it and the German hackers, at any rate, support a drug-based lifestyle on their activities. I was about to say, 'enjoy', but I should certainly not enjoy a lifestyle based on drugs. Because drugs are expensive, hackers need to make a great deal of money to support their lifestyle (Nicholson, Hansard Feb 9th March 1990: 1154).

Nicholson fails to give any corroborating evidence for many of these assertions. Her association of German hackers and drugs is possibly a reference to the case of Pengo, the hacker Stoll tracked down in The Cuckoo's Egg, but that individual case does not seem to warrant the status of being generally applicable to the whole German hacking scene. This example of lack of specific evidence raises the question of the information gap regarding computer crime that policy makers are faced with. The disproportionate reliance upon the 'casual empiricism' of rumour and 'guestimates' increases pressure to legislate against hacking because of the increased levels of fear the lack of statistics may produce: "while we are aware of the tip of the iceberg, we do not know how much lies beneath the surface" (Waller, Hansard Feb 9th 1990: 1161).

(ii) The information gap in parliamentary debates

In the parliamentary debate, Nicholson exemplifies this tendency of reliance upon rumour by refering to the unsubstantiated 'casually empirical' case of Scottish poll tax computers having had details of those eligible substituted with information of dead people. Waller demonstrates the role of 'guestimates' with observation that 80% of the computers in Hong Kong have been infected with at least

one kind of virus. The Internet worm is an example of a computer intrusion incident which recieved large scale attention and suffered a similar exaggeration, this time more specifically as a result of press interest:

> The incident received world-wide press coverage. Along the way the extent of the damage was magnified. One of the first estimates- from John McAffe, the ever-quotable chairman of CVIA - was that cleaning up the networks and fixing the system's flaws would cost $96 million. Other estimates ran as high as $186 million ... McAfee's estimate of $96 million was dismissed as being 'grossly exaggerated' by Cornell University's subsequent report on the incident (Clough and Mungo 1992: 98).

The vagueness of figures relating to computer crime appears to be a common quality compounded by the boastfulness of some hackers, and also stemming from a reluctance of the victims of the crimes to report their vulnerability. This produces subsequent difficulties when trying to collate reliable and meaningful data about security breaches. Dr Taylor gave the follwing account of this:

> There's lots of media hype but it all comes back to the number of facts and occurences, what I'd say is that there are very few virus incidents that are discussed in public which is due to a very simple reason. If ... a company gets hit hard with a virus because somebody's been negligent in checking for example in-coming discs or in-coming software, then the next time there's a general meeting of that company, then all the share-holders of that company will go for the chief-executive or his henchmen and just roll the lot of them and put in a new board. It's a job-losing incident, so whenever there's a security incident not just involving viruses, anything involving hacking, fraud, forgery in any plc which has got public share-holders, there's a big white-wash job done ... I would say, I've got to guess, but I would say there's probably 10-20 serious security incidents in public companies a year, all of which are white-washed, otherwise the management are accused of negligence (Taylor: Knutsford interview).

In summary, the wide-spread reliance on 'guestimate' figures, in the press and trade journals, results from a reluctance to report incidents. This exacerbates fears by exacerbating perceptions of the potential harm hackers can commit, which then contribute to the 'them and us' stigmatisation process and the concomittant sense that a legislative response is required to solve the problem.

7.7 ISSUES IN COMPUTER MISUSE LEGISLATION

Amongst the problems faced by computer misuse legislators, is the problem of attempting to interpret the motivations of hackers - the legal question of intent, and there are also various difficulties encountered in the previous chapter of how to transpose real world concepts into 'virtual reality'.

(i) Interpretations of motivation

> *Everything is so ill-defined. How can you guess what lies in their hearts if you can't see their eyes? How can one be sure that, unlike Mitnick, they won't cross the line from trespassing into another adolescent pastime, vandalism. And how can you be sure that they pose no threat when you don't know what a threat might be?*" (Barlow Fall 1990: 14).

The question of intent is obviously important when it comes to framing legislation to deal with the perceived problem of hacking. The Computer Misuse Act attempts to distinguish between the different possible motivations of hacking. It imposes maximum sentences of six months for harmless browsing and five years for "unauthorised access with **intent** to commit or to facilitate the commission of a more serious further offence, such as fraud or blackmail" (Colvin Hansard Feb 9th 1990: 1138).

The crucial difficulty faced by legislators is that they face the danger of being accused of excessively punishing and labelling people as criminal, when their 'crime' is liable to perceived as relatively 'innocent' computer browsing. Chet Laughlin, for example,

gives the scenario of a "14 year old hacker-wanna-be" who largely through luck gains access to a system and uses the opportunity to browse through it. In such a case "pressing for time behind bars for this (strawman) seems overkill. Now perhaps if I can demonstrate a DESIRE TO DESTROY or MALICIOUS INTENT I could see otherwise" (Laughlin 1991: Risks 11.34). Thus, even if it is accepted that computer intrusion is wrong, achieving widespread agreement that hackers are criminals in the traditional sense, is arguably much more difficult. The dichotomy faced by legislators in the case of computer crime is that to successfully label hackers as criminal requires proof of malicious intention, whilst the anonymity afforded by the medium of computing often makes such a task extremely difficult to achieve. This has not stopped attempts being made, however, and in the following description of the Atlanta sentencing of Riggs[6] and his associates, the process of marginalisation at work in a specifically legal context can be seen:

> Although the prosecution concedes that '[the] defendants claimed that they never personally profited from their hacking activities, with the exception of getting unauthorized long distance and data network service,' the prosecutors nevertheless characterize the hackers' motives as similar to those of extortionists: 'Their main motivation [was to] obtain power through information and intimidation.' The prosecutors add that 'In essence, stolen information equalled power, and by that definition, all three defendants were becoming frighteningly powerful (Thomas CuD 2.07).

The fraudulent underworld described previously by Gongrijp is an example of the more obviously criminal aspects of the computer underground. It becomes less easy to interperet the correct legislative approach to adopt, however, when the 'crime' being committed is limited to non-destructive, but illicit use of someone else's computer system. Kevin Mitnick, pointed out to me the likelihood that in many legal cases a judge would have to use his/her discretion as to whether an act was committed with criminal intent.

[6] c.f. Fig. 7.1

Harry Onderwater of the Dutch Criminal Research Institute in The Hague concurred with this idea. He also outlined his perspective on how, even accepting that hackers are criminal, there is still room for differentiations to be made:

> I think there are some good hackers and a lot of trained monkeys as they call them. What they do, it's very easy by internet, you connect to a site and say system administrator or system manager, test, test, they know that you can ... and that's not hacking, that's the difference between a burglar who puts a big crow-bar between a door and the guy who's picking the lock. He's a specialist and he doesn't break your door, if he meets the night-watch, he wouldn't kill him or hit him, it would be his risk. There's quite a difference between those guys ... there's a difference between the guys who are worth the knowledge and who know what they are doing and trained monkeys ... If you get a Dutch data-base you can enter a lot of sites because the other people already, the specialists, already found it out for you, and that doesn't make you a good hacker (Onderwater: Hague interview).

Even though people such as Onderwater can recognise the differences between technically 'good' and 'bad' hackers: the 'specialists' and the 'trained monkeys', those involved in both the practical prevention and the legal prosecution of hacking are, perhaps inevitably, much more concerned with the effects of hacking than the original motivations behind it. This forms an important element of the "them and us" situation. The CSI thus generally works on the assumption that the motivation of all hackers has to be viewed as if it was criminally-induced. The argument is that there should be no differentiation made between the different motivations of various forms of hacking. Although hackers such as Mitnick request recognition of these differences, security people such as Thompson, Taylor and Tozer emphasise the fact that the effects of hacking, potential or actual, can be damaging regardless of the original motivation or intent, and that therefore legislation should seek to eliminate hacking regardless of its intent.

This call to treat as unimportant differing motivations was reiterated by MP's. One rationale centred upon the line of argument that victims of intruders, once aware of an intrusion, are obliged out of caution to treat it as being maliciously inspired, the law should therefore back this socially responsible attitude by treating all hacking as legally punishable:

> The issue is whether criminal law should be available for trespass into computer systems. We must remember that trespass is criminal in certain circumstances ... For example, statute law makes trespass criminal where trespass occurs on certain property and in particular on British Rail property ... Similarly, it is a crime to trespass on certain property if no damage is done, but firearms are being carried or is someone trespasses in pursuit of gain ... I believe that computers should be the kind of property on which to trespass would be criminal, because of the damage that such trespass can cause (Cohen, Hansard Feb 9th 1990: 1178).

Trespass is not seen as being strictly analgous to computer trespass because it does not normally give rise to actual physical damage, the damage caused by computer trespass stems from the obligation to check for damage it forces upon the owner of the system. The parliamentary debate over the Computer Misuse Bill reflected the concerns regarding the question of intent:

> The Bill criminalises the act of unauthorised access to a computer, irrespective of the circumstances in which that is done. A person might access a computer to read something that he could obtain in a library-for example, a Shakespearian sonnet. Such an act will become a criminal offence subject to six-months' imprisonment. By contrast, an unauthorised person who reads the most sensitive manual files can get away with it, but such action is far more offensive (The Independent: p.4, 15 July 1993).

He points out that the fact the Bill does not uncontroversially deal with the subject of intent is shown by the close 3:2 outcome of a British Computer Society debate, which occurred in a committee

room of the House of Commons attended by 130 comptuer specialists between, amongst others, Miss Nicholson and Prof Brian Niblett a Home Office computing adviser. The division within the establishment over the implications of the Bill are further highlighted by the view of Mr. Eric Howe, the Data Protection Registrar:

> Mere misbehaviour, for example by youngsters, is not a matter which we normally would seek to criminalise unless it has some significant effect. To criminalise all unauthorised access or attempts at access regardless of whether there is damage or risk of damage would be to take a serious step which I find hard to justify as a matter of principle. I believe that it would be wrong to criminalise those who have no criminal intent and create no hazard. This is analgous to a case of trespass where no damage is caused. There may be a case, however, for dealing with persistent unauthorised access. We should not lose sight of the fact that computer users ought to protect their own systems ... you've only yourself to blame if your neighbour's cattle get into your unfenced field (Cohen, Hansard Feb 9th 1990: 1166).

There is a worry that anti-hacking legislation will exacerbate lax security rather than aid attempts to improve it. Quoting a computer conferencing speicalist, Terence Wright, Leigh contends: 'The great Prestel 'hack', which is so often cited, was a case of a wide-open door, and not of security being broken. There was no security and there should have been." I hope the Bill will become an Act, but no one would want it to absolve people in the computer industry from being responsible for closing doors. That is their responsibility" (Hansard Feb 9th 1990:1171). The veracity of this statement would seem to be underscored by the way in which Robert Schifreen, one of the perpetrators of the hack, has previously been quoted describing the poor level of security that allowed his largely serendipitous intrusion to occur at all.

The problems of assessing the intent behind a computer intrusion are exacerbated by factors that have been emphasised throughout this study. One of these factors is the cultural difference

between those implementing legislation and those most likely to be affected by it, previously identified by Herschberg as stemming from the fact that hackers have grown up with computers 'from the cradle'. Mr Leigh MP argues: "There is a wide cultural gulf between those who learned computing in 1961 and those who learned in childhood more recently.' Is my hon. Friend ... (Miss Nicholson) able to distinguish hitting keys 1980 style from hacking? Can the courts? Will they convict the innocent because they did not do what the manuals said they should do?" (Hansard Feb 9th 1990: 1171).

(ii) Non-applicability of conventional concepts in cyberspace

The non-transferability of virtual world concepts to the real world identified particularly in Chapter 6, contributes to legislative problems. 'Disembodied' is a phrase the Michalowski and Pfuhl (1990) use to refer to computer-based crime in their discussion of the formation of computer crime laws. It is a phrase that aptly describes the consequences of the growing immateriality of information. One implication of this is that the act of attempting to illicity access and use such information does not fit neatly into existing laws designed to deal with traditional notions of theft:

> In one such lament, Business Week claimed that even if information thieves are caught 'it is not always easy to prosecute them. Larceny means depriving someone of their possessions permanently. Can a person be tried for stealing a copy of information when the supposedly stolen information remains in the computer?' Similarly, Mano complained, that one 'might as well play billiards with a sash weight' as try to control computer abuse by applying existing laws to this new threat (Michalowski and Pfuhl 1990: 268).

The basic problem which the authors identify is that society is finding it increasingly difficult to protect traditional property rights, in the realm of computing, due to the qualitatively different features of electronic data storage. In the face of these problems, Gongrijp

contends that the establishment response to computer crime has involved a disproportionate and unjustified strength of reaction when compared with similar real world crimes. This over-reaction occurs, he claims, because whereas normally within the justice system the intentions of the defendant are an important part of the alleged crime, the same allowance for motives is not made with incidents involving computers:

> you can steal a document in a company, photocopy it and take it home, and they could do nothing, maybe within the company, but there would be no criminal offence, within the company they could fire you. And then if you do the same thing with a computer it should be a criminal offence, why? In all the rest of the justice system it depends on what you do with them [documents or whatever], it depends on your intentions, and as soon as you use a computer, your intentions are no longer important, it's just that you use a computer, it's a magic area that we don't understand and that we can't control so that we must take you one step before you do harm and we must not care about your intentions: it's bullshit! (Gongrijp: Amsterdam interview).

This forcefully expressed opinion highlights some of the difficulties encountered in the transposition of legal concepts to computing. For some hackers, the problems encountered in legislative approaches are indicative of the fundamentally misguided nature of the attempting to make this transposition: "If we succeed in convincing people that copying a file is the same as physically stealing something, we can hardly be surprised when the broad-based definition results in more overall crime. Blurring the distinction between a virtual infraction and a real-life crime is a mistake" (Goldstein CuD 5.43: 1993).

In keeping with Goldstein's assertion, attempts to create legislation aimed at facilitating the blurring have encountered various anomalies. Cohen points out that Alistair Kelman a barrister specialising in computer law has queried why non-malicious browsing should become a criminal offence, in terms similar to those of Goldstein he warns that: "The Bill's net is being cast far too wide,

and it will lead to many people, some vulnerable, committing a crime where none now exists ... In years to come, the Bill could apply to a washing machine, controlled by a chip ... That is nonsense" (Hansard Feb 1990:1166+7). It has been argued that the Bill inherently lacks focus: "Are we really saying that members of staff who make unauthorised use of a firm's personal computer to produce their own CV or every perpetrator of a childish prank that their misdemeanour is worthy of a criminal record they will keep for the rest of their life?" (Leigh Hansard Feb 1990: 1173). Such anomalies result from The anomalies encountered in the literal transposition of real world criteria into 'virtual reality', are both caused by, and subsequently exacerbated by, the rapidly changing nature of computing. The speed of this change is such that there is no point within The Computer Misuse Act where the phrase 'computer' is actually defined. Colvin, the MP who brought the Bill before the House, claimed: "The problem is that it was six weeks ago when I first defined the word 'computer' to my satisfaction. That definition is already out of date. The passage of time and the pace of development within the computer industry mean that any definition of a computer or a computer system would soon be out of date" (Hansard Feb 1990:1159).

(iii) Deterrence

There are various problems stemming from the fact that it is effectively impossible to know, a priori, the intent of an intruder 'cloaked in electronic obscurity'. Legislation, therefore, instead of aiming to be efficient in terms of retributive justice, may have to focus on the limited aim of acting as a deterrent. Even this more limited aim, however, may be difficult to achieve. Zmudzinki, a system manager on a military site, put forward the following argument about the effectiveness of computer misuse legislation with reference to the actions of Robert Morris:

> The law is ... an ass. At the time I thought he should have gotten two years with a roommate called "Bubba". Now I'm not

so sure. The problem is that most legal systems are based on the concept of punishment as a deterrent. This assumes that one is dealing with persons of adult viewpoint. Unfortunately, adolescents are not adults by definition. [I've always like the definition of 'adult' Bob Heinlein gave in The Moon is a Harsh Mistress: An adult is a person who has accepted the inevitability of his or her own death. (There are a lot of "tall children" running around.)] The point is that when one is dealing with people who truly believe it-can't-happen-to-me, deterrence fails (Zmudzinski: e-mail interview).

This is a view backed by fieldwork evidence of hackers experiences:

> Laws really don't mean anything to hackers until they get caught. They might consider them to the extent that they will not give out their number, or use an alias, or try to hide their call routing through a number of paths, but they don't really care. It's akin to jaywalking, it's illegal, but the law is considered as an inconvenience to the offender (Eric Coggans: e-mail interview).

Kevin Mitnick argued:

> I don't think they're doing it because it's against the law and they want to break a law, they do it because it seems an interesting thing to do, a very interesting thing to do and it just happens to be against the law, but, tough. Speaking for myself, I was into computers, I wanted the knowledge and I was very interested, it wasn't totally against the law in my day, it was a very grey area, but I wasn't doing it because it was a kick because it was against the law, I was doing it because I wanted that knowledge and it just so happened to be against the law, but I would have done it if it was legal or not (Mitnick: telephone interview)

Mike Jones, is a member of the DTI's security awareness division, and as such, was instrumental in the drafting of the 1990 Computer Misuse Bill. In contrast to Zmudzinski, he thinks that legislation, at least in the British experience, has in fact dampened

down, at least temporarily, hacking activity, and does act as a useful deterrent:

> I would like to see no prosecutions at all and hacking stop, but I recognise that we live in the real world were hacking will continue just as theft and murders continue, but that ideally, the Act will provide a greater deterrent to hacking than previously obtained. To provide a deterrent I think the Act has to be used not only in threat but inevitably it has to be used in anger ... so inevitably, there will have to be prosecutions, how many I don't know, maybe two or three a year would be sufficient to provide the level of deterrrence, I don't know maybe one would do it ... I've spoken to senior spokesmen in the Metropolitan police, who argue that hackers are now lying low, they might still be waiting, they haven't given up hacking altogether, but they're just looking to see which way the cat will jump basically (Jones: London interview).

That the threat of jail sentences for what was previously considered to be an act of intellectual fun-seeking has contributed to a tense atmosphere within the CU is shown by Maelstrom, who, after recounting the diversity of his previous hacking exploits, admitted that:

> Now I spend most of my time here at the college learning VMS on my legal accounts. I still have fun getting into computers on other campuses, but I don't really have the time I did before I started college. Many of my close friends have gone to jail or have quit the scene, so the inspiration to come up with neat hacks has also died down a little (Maelstrom: e-mail interview).

The emphasis the CSI placed upon the more psychologically-disturbed members of the CU[7] in the formation of legislation is viewed by the CU as irrelevant to the extent that it fails to address the underlying thirst for knowledge and access to systems motivating 'responsible' hackers. The CSI is perceived as simultaneously over-emphasising the extent to which hacking

---

[7] E.g. Dr Taylor and Mr Tozer of the BCSSC and their accounts of Chapter 5.

activity is dominated by vandals, whilst unrealistically wishing or believing that such vandals can be eliminated from their systems:

> Should all responsible hackers be scared off by the militant action of security people, it would seem obvious that the security people would have much, much more to worry about ... Fantasizing about the absence of vandals is no different than wishing for the disappearance of all drug dealers. Basing argument upon such fantasy is beyond comment. I venture a guess that most security people are not the brightest of fellows because even one who is as twisted as I, can see that malicious and vandalous acts perpetrated in any environment, whether it be in the slum or in a VAX, are the result of many factors not having anything to do with computers. Addressing these causes and making education available is where resources should be dedicated. If individuals didn't need to break into computers to quench their thirst, either for knowledge or for malice, then certainly it would not take place as often (if at all) (Mofo: e-mail interview).

Mofo thus raises the issue of the potential policy implications resulting from loosely associating vandals and hackers together. A failure to distinguish between them is part of the stigmatising process that signifies the CSI's attempt at closure; all hackers are grouped together under the label of 'vandals'. Such stigmatisation serves the purpose of reinforcing the CSI's group identity, yet risks constituting a misdirection of resources if the ultimate aim is to eliminate hacking. The implication from Mofo's view is that punitive responses to hacking are likely to leave unaffected those motivated by destructive and malicious intentions, thereby severely limiting the effectiveness of the deterrent qualities of computer misuse legislation.

(iv) Symbolic value

Such legislation as the 1990 Computer Misuse Act may have deterred some would-be hackers. However, as we have seen, considerable doubt remains regarding its role as a deterrent and

further doubt has been expressed as to whether such a desire to deter was the main motivating force behind the legislation in the first place. This adds weight to the symbolic view of computer misuse statutes. A specific charge relates to the scant resources available if the Act is likely to be enforced:

> I hope that the Minister will deal with the problem of enforcement. We are reminded that out of 150,000 police officers in England and Wales only five are mainly concerned with computer crime ... Fewer than 100 have received even the minimum four weeks basic training and the Serious Fraud Office has one computer-knowledgeable official (Leigh, Hansard Feb 9th 1990: 1172).

Claims that the Computer Misuse Act is largely a symbolic measure are also inadvertantly supported by some of its own proponents who question the likely efficacy of the Bill whilst affirming the sentiment behind it. This is a characteristic of symbolic legislation (and to a lesser extent most legislation): that it should espouse a particular social message irrespective of the law's likely ability to enforce that message. An example of this characteristic is Moonie's questioning of whether the Bill will provide adequate deterrence:

> It may deter the occasional recreational hacker, but the seriously disturbed person who perpetrates serious offences may not be adequately deterred by it. People will not be deterred if there seems little chance of being caught ... Will inventive minds find some way of circumventing the Bill? I hope that it's drafting is secure enough to prevent that. I support the Bill in principle. Its internal structure is sound, but it is a matter of conjecture whether it will do what it is purported to do (Moonie Hansard:1160).

The quantitative questionnaire also illustrated the doubts people have as to the likely efficacy of legislation, at least in its existing form, in reducing the incidence of security breaches. This is shown in the table below which summarises responses to a question from the fieldwork's quantifiable survey, about future changes in the

level of security. The vast majority of respondents (73%) felt that security breaches would increase.

Q 25: What do you think will happen to the future level of security breaches?

Fig. 7.1

	Frequency	Percent
viruses will increase/ system breaking decrease	1	0.5
increase	146	73.0
decrease	14	7.0
stay the same	39	19.5
Total	200	100.0

The above factors suggest that the justification of the Computer Misuse Act on the grounds that it will reduce security breaches by its deterrent effect on hacking is open to criticism. In addtition, the statistics from Chapter 5 imply that the Act may be of limited effectiveness because it over-estimates the significance of hacking as a security threat. Whilst the Act applies to those misusing computer resources inside an organisation, as well as hackers, it's efficacy in this situation is likely to be reduced by the fact companies fearing adverse publicity are more likely to take internal disciplinary measures than resort to prosecution under the Act. The charge that the Act is more symbolic than a real deterrent is also strengthened by the belief that the timing of the Bill's introduction had more to do with a desire to be seen to be doing something about the problem,

rather than a sudden realisation that there was a problem in the first place:

> Arguably, any need to deter abuse existed long before the enactment of computer crime statutes. In fact, the available data suggest that serious economic losses linked to computer abuse have been and continue to be attributed to current and former employees of the victimised organisation rather than to interloping hackers with modems. The temporal lag in the criminalisation of computer abuse (not observed with the introduction of other technological changes), seriously challenges the extent to which the computer crime laws can be understood purely as instruments of classical deterrence (Hollinger and Lanza-Kaduce 1988:116).

The classical deterrence view, however, still seems to hold sway in the mind of the legal establishment. In the same case that Paul Bedworth was acquitted, two of his codefendants were sentenced to prison terms. The judge explicitly stated that his sentencing rationale was based on the desire to deter other hackers. In his summing up he said:

> If your passion had been cars rather than computers we would have called your conduct delinquent, and I don't shrink from the analogy of describing what you were doing as intellectual joyriding ... There may be people out there who consider hacking to be harmless, but hacking is not harmless. Computers now form a central role in our lives ... Some, providing emergency services, depend on their computers to deliver those services. It is essential that the integrity of those systems should be protected and hacking puts that integrity into jeopardy'. He said that hackers need to be given a 'clear signal' by the court that their activities 'will not and cannot be tolerated' (The Independent pg4, Saturday 22 May 1993).

It is impossible at this early stage of the Act's existence to evaluate its success as a deterrent. Judging from the difficulty I encountered in trying to interview British hackers or presently active American ones, it would seem that at the very least, the legislation has discouraged the hacking community from carrying on

their activity, or discussion of it, "above ground". The accompanying assumption is that unless the deterrent effect of the Act has been large, then it has served to drive most hacking activity 'underground', which as we shall shortly see, creates its own associated problems.

7.8 PROBLEMS OF ENFORCEMENT

(i) Problems of Enforcement

Because of the electronic basis of their activity, hackers are an elusive and largely anonymous target for law enforcement agencies. Even assuming that they can be caught, achieving a punishment likely to provide a deterrent for other hackers has proved difficult. The problems associated with enforcing computer misuse legislation are illustrated in the table below:

FEW VICTORIES IN THE WAR ON HACKERS

SUSPECT	ALLEGED CRIME	OUTCOME
Robert Morris Jr.	Convicted of breaking into and crippling a national network of government and university computers	Sentenced to probation and community service
Steve Jackson	President of computer-game maker company accused of publishing "a handbook for computer crime"	Case dismissed because of lack of evidence
Craig Neidorf	Accused of publishing classified phone company information in his electronic newsletter	Case was dismissed when information was shown to be publicly available
Franklin Darden Adam Grant And Robert Riggs Jr.	Convicted of conspiring to defraud BellSouth[8] of information and disrupting telephone services	Each sentenced to a year split between a halfway house and probation
Leonard Rose Jr.	Pleaded guilty to transmitting stolen AT&T Software	Agreed to serve one year in prision

(Stockfield, 1991:62)

Fig. 7.2

[8] U.S. telephone company.

(ii) Legal complexities - the Bedworth case

The case of Paul Bedworth illustrates several of the problems encountered by the Computer Misuse Act in the sense of both drafting and enforcing computer misuse legislation. The fact that the case of Paul Bedworth ended in an acquittal despite unequivocal evidence that Bedworth had gained illegal access to numerous computer systems raises doubt as to whether the Computer Misuse Act will function efficiently as a means for both deterring and punishing hackers. It would seem that society's response to hacking is still of an ambiguous nature: even where uncontested evidence of computer hacking can be produced (and this itself is often extremely difficult to do), a conviction under the relevant legislation is not guaranteed. This points to both the legal difficulties encountered in trying to combat hacking, and also the general ambivalence of the public's response to it: for example, the jury only took 90 mins to come to its decision, despite the complexity of the case and the fact that the prosecution's case had involved two years of work involving police from eight separate forces. One of the possible reasons why "the perverse verdict" was passed is due to the fact that the Bedworth case exemplifies the problems of attempting to enforce a generic law over computing situations that vary significantly according to each individual case's particular circumstances and which are subject to the above-noted problems of being able to apply adequately, real world concepts onto the realm of computing.

There is, for example, a tendency to couch computer misuse-orientated legislation in broad terms so as to avoid legal loop-holes that can be exploited by defence councils. Because of the difficulties of pinning down a stereotypical hacking method of entering a computer illegally, the Act prohibits generic "unauthorised entry" with the subsequent problem that too much computer activity will then tend to be inadvertantly included within the provisions of the Act. Despite the determination of the Act's drafters to ignore the "benign intent" defence of harmless browsing, the issue of intent remains important to juries. The underlying malice or harmlessness behind a computer intrusion becomes the yardstick by which juries

assess hacker trials. They may find it difficult to attribute malicious intent to hackers faced with the immaterial nature of their activity. Because hacking exists in a "virtual reality", what the law seeks to label as criminal intrusions, tend not to have the same criminal associations real-world physical intrusions would have:

> somehow over the period of the 16-day Southwark Crown Court "show trial", as the defence described it, the scrawny, wan 19-year-old has always seemed an unlikely villain...All three charges faced by Mr Bedworth were couched as 'conspiracies' But, the defence asked, can conversations with other teenagers over computer chat lines really be said to constitute a conspiracy, or was Mr Bedworth operating largely alone, and just swapping the odd tit-bit of information with modern-day pen pals? (editorial Independent 18.3.93: 4).

It is doubtful whether the technical ignorance of the jury can be used as an excuse for the reluctance of people to categorise hacking as a tradtional crime. The psychologist Mary Shotton typifies the reluctance of even professional groups with interests in the question of hacking, to label hacking as a criminal activity (using language remarkably similar to that quoted above by Zmudzinski). She contends that, "Most people who hack are aware that it is a bit unethical but they see no reason not to do it. They are far from stupid. They think the law is an ass. I would rather have a hacker as a son than someone that ram-raids or joyrides ... you could argue that hacking is safer, saner and more intellectual" (Nutall 1993:5).

7.9 LEGISLATION AND THE EVOLUTION OF HACKING: MIT TO ALCATRAZ

The charge that legislation is largely symbolic may also result from the apparently inevitable bind that legislators face when seeking to produce a legal framework within which hacking can be contained. They can be accused of attempting to 'shoe-horn' computer security cases into existing but allegedly unsuitable laws, or alternatively, they can be accused of producing new laws that

misapply traditional concepts such as theft and privacy to the qualitatively different world of computing. Because of the relatively recent appreciation of the problem of computer security and its implications for computing and society, many of the complex legal issues remain to be resolved through the usual processes of legal debate and precedence. Chapter 5's treatment of the technical aspects of hacking has shown security weaknesses to be a part of the inherent fallibility of human-designed systems, and that given sufficient perserverance and technical knowledge on the part of hackers, bugs and software faults can be used for purposes other than those intended by the original designer. The basic problem facing legislators, therefore, is how to design a legal structure that will deter such illicit uses from occurring whilst avoiding the potential risk of marginalising "benign" hackers, with legislation, so that their knowledge and perseverance is herded towards more orthodox and traditional criminal groups:

> Today we are faced with a new breed of vandal. In the past 3 years I have seen the emergence of real computer thugs. These people are from low-class areas who have immersed themselves into the computer networks and look at hacking as a means to control their environment. Hacking to them is more than intellectual fulfillment, it's an ego trip. Where people like myself learned and moved on, these people learn and abuse for their own gain ... I think that the computer underground as I know it will be gone very quickly. It will be replaced with a TRUE criminal underground. The technology is slowly reaching the baser elements of society who are using it for their own benefit. Hackers as we know them will be gone, washed out with the implementation of laws, and technological advances to prevent casual break-ins. The only people who will be intruding into computer systems will be doing so with ulterior motives (Coggans: e-mail interview).

The above quotation exemplifies some of the perceived dangers confronting computing from the allegedly increasingly criminal nature of hacking activity. Understanding the motivation behind hacking activity and the differences between "responsible" and

"vandal" hackers is seen by the CU in particular as necessary in order to target resources to the real causes of hacking without alienating "responsible" hackers who may prove to be a useful resource in limiting the destruction of the vandals. The predisposition of the CSI to group non-intentional and intentional damage together, would seem to increase the tendency towards the criminalisation of hacking whatever its underlying motivation. A view warning of the dangers of criminalising hacking, was voiced by Dr Cohen, who argues that the main motivating cause of hacking is the desire to explore that is common in teenagers irrespective of computing technology:

> We can either treat it as healthy and provide a venue for it, or turn our children into criminals by criminalizing their normal behaviour ... When I was younger, I knew many "hackers" who went after systems, and none of them were malicious. Now I know some malicious ones, but they are generally malicious because of family or financial problems, not because they are "criminals". In every case I have seen, these people need friends and legitimate ways to explore. They need guidance and moral interpretation from someone they respect, not jail time with rapists and thieves in some stinking cell ... As the group ages ... people begin to cross the line between explorer and pirate. Unfortunately, many of these latter day Fagans corrupt young people who, in their quest to explore, are not given legitimate venues, and are thus drawn into illegitimate activities ... the reason most of these people are drawn into the "dark side" is because they are abandoned by the "good guys". I for one, will not abandon our youth to criminal acitivities (Cohen: e-mail interview).

This view reinforces Mofo's claim that the CSI should be more concerned with the "access" and "thirst for knowledge" causes of hacking. Targeting resources in these directions is arguably more productive in the long run than the risk of provoking 'militant' CU acts of vandalism with hawkish, unsympathetic responses. This argument gains some credence when one looks at the existence of "virus factories" in the former Eastern Bloc countries, largely as a result of a lack of useful alternatives for programmers' computing skills.

The reponse of the CSI to hacking activity is crucial in determining the uses to which much hacking knowledge will eventually be put. The fear that by placing hackers in prison such knowledge will be directed into the criminal community is also expressed by 'Mofo' who also uses the example of the Internet Worm. He contends:

> There were individuals who would have Mr. Morris be quartered in an actual prison. Such puerile reaction! I myself was in a position to demand that Mr. Morris receive capital punishment AND a fine, but reason seems to have eventually prevailed in my muddled mind. I present this observation: an intelligent person sent to prison for such an act would certainly come to the conclusion that society demands his/her subsequent interaction with the denizens of such an institution. Thus, I believe that society as a whole would be far better off if the intellect of a person like Mr. Morris was not shared and information not disseminated among hardened criminals with truly malevolent intent (Mofo: e-mail interview).

In keeping with this scenario, there is the example of Nicholas Whitley known as the 'mad hacker':

> The only times Nick Whitley was ever approached to do something he thought was illegal was when he was already in jail. The first attempt was made in the exercise yard in London's Brixton prison: Whitely was a hacker, wasn't he? He could break into computers, right? Well couldn't he break into the Police National Computer and change a few files? It would be worth £10,000 to some people to have their police records deleted. Nick declined (Clough and Mungo 1992: 42).

The experience of hackers such as John Draper, who have served prison sentences for hacking further illustrates some of the problematic implications of imprisoning hackers:

> In most cases, criminals hackers might meet in jail or prison are too stupid to understand the ramifications of hackers' information. Lately, however, a lot of newer prisoners have been added to the usual murderers, drug dealers, thiefs, etc..

> These are embezzlers, fraud artists, scam artists, and other "sharks" that wouldn't hesitate for a moment to capitolize on hacker technology to enhance their scams ... Your academia experts may know a LOT of things, but until they actually EXPERIENCE inmate life in jail, they will NEVER EVER know what really goes on in prisons ... In MY experience, when I was released, almost everyone I had contact with in prison has since contacted me after they also got released. Some have even offered me large sums of money to hire me as a consultant ... In most cases, those hackers approached by ex-cons will be offered huge sums of money as an incentive to "spill the beans" and teach hacker technology, so a hacker will be most patient, even though they are talking with a moron. Eventually, even the dumbest moron will catch on to the automated techniques of breaking into systems (Draper: e-mail interview).

There is, therefore, an indefinite boundary lying between the boredom and frustration felt by some adolescents who feel they have inadequate access to computing facilitites, and the criminal activities that may result from such boredom. There is on the one hand a need to deter troublesome hacking activity, yet to criminalise such activity has potentially dangerous and counter-productive consequences.

7.10 CONCLUSION

Draper's account of his prison experiences points toward how the gap between the CSI and CU's knowledge of security weaknesses may become exacerbated if hacking knowledge is driven further underground and into the prison system. Draper's observations would seem to reinforce Dr Taylor's warnings of hacking technology becoming more widespread, and hacking knowledge being passed down criminal information networks, yet they also seem to imply that such a process would be speeded up by legislation against hacking. To avoid this problem, there is a need to devise a legislative approach which would successfully reflect different and appropriate legal approaches for the various motivations that may lie behind

hacking activity: whether this is possible, is yet to be seen. There remains, however, a practical need for legislators to develop a thorough understanding of the motivations which lie behind hacking, both malicious and non-malicious, if future legislation is to prove effective in dealing with the problem both as a deterrent and as an effective means of enforcing retributive justice.

Investigations into the formation of legislation aimed at computer crime emphasise its symbolic characteristics. Its primary aim is seen as not so much to be efficacious, but rather, to serve the political aspirations of its promoters. If such claims are true, then there is ground for substantial concerns about the future development of computing. This chapter delineated the various anomalies associated with attempting to use existing legislation, or new laws, to deal with what are arguably qualitatively new situations engendered by computing technology. These anomalies may not be assimilated adequately into new legislation. There is pressure to enforce ultimately unsuitable, but established ethical codes and property rights in order to create and maintain boundaries between groups in a nascent industry. In addition, there is a perceived need to enforce these ethical codes in order to defend the status quo of a societal order threatened by the disruptive technological innovation of computing.

The implications for the development of computing of the above scenario, become potentially more harmful if it can be shown that new legislation has not adequately addressed the conditions within the computing industry that allow the possibility of hacking in the first place. Thus if legislation against hacking becomes more draconian, yet computer security remains inherently weak, there is the danger that hacking knowledge will be driven further underground into professional criminal elements, and that the overall effect of legislation will have been counter-productive to the original aim of reducing the threat posed by hacking. It may in fact become more destructive, whilst at the same time, fear of prosecution may reduce the numbers of cooperative hackers willing to help draw attention to security weaknesses.

The tendency to punish all hackers, irrespective of motivation, as a result of the problems of establishing a priori intent, raises various legal problems. Firstly, the precept of "innocent until proven guilty" is threatened, and secondly, in the desire to punish all hackers, the particular anomalies and complexities of cyberspace are largely ignored, and conventional legal concepts are consequently misapplied to the realm of cyberspace. Examples of this are the problems encountered when attempting to transpose the legal concept of "breaking and entering" onto concepts of computer misuse: any act of computer intrusion and subsequent "theft" is most likely to leave the "stolen" object remaining in the breached computer. Attempts to impose proprietal relations onto computing activities are confronted by opposition, caused, not by a wilful desire for illegality, but rather, the sheer convenience of using technology illicitly. A conflict occurs between informational exclusivity and the benefits of flouting it.

The statistical evidence relating to computer crime further complicates the issue of legislation. The existing data is used both by those claiming that legislative responses are largely symbolic, rather than effective, as well as by those who argue that the figures justify legal responses aimed at reducing computer crime. This study shows that from the most extensive research performed to date, the financial costs of hacking are relatively small compared with more prosaic threats such as user-error and insider-based fraud. Advocates for legislative responses, however, emphasise the fact that available crime figures may be understated due to companies' fears of adverse publicity.

Despite the rationale for legislation, commentators tend to be sceptical of its likely success in significantly reducing the incidence of hacking. They compare legislative attempts to King Canute trying to order back the waves, or to playing billiards with a sash-weight. Both those advocating and opposing the legislative solution to hacking emphasise the fine dividing-line that exists between a hacker enjoying a particular form of intellectual curiosity and him acting upon the criminal potential the activity holds. The more hawkish attitude is that hackers are already liable to change into a

criminal 'in an instant' and are thus suitable subjects for criminal legislation. The more dovish response portrays society as being on a cross-roads whereby hacking in the form of intellectual exploration can be encouraged, and remain predominantly benign, or criminalised and liable to become more malicious and destructive. The latter course is criticised on the grounds that it is penalising the innate intellectual curiosity of adolescents and pushing them towards the conventional criminal underground. The account of the prison experiences of hackers such as Draper seem to add weight to fears that hacking knowledge could be utilised by those with ulterior motives, who although they may not be particularly technologically able, will still be able to make use of automated intrusion techniques.

The overall significance of the Computer Misuse Act is that unlike other forms of legislation, such as that relating to the wearing of seat belts, this particular legislation is not just seeking to convey an ethical message, the sentiment of which most people can agree with, but it more specifically seeks to create a particular climate of opinion by which a group within society (in this case hackers) can be marginalised. Ultimately, what separates hackers from the CSI is the manner in which they choose to underline how the technology of computing creates new communicational possibilities and ethical situations, and arguably these should not be judged using a rigid application of "real world" notions that do not fit cyberspace. Legislation to enforce informational exclusivity is viewed as the latest course of action in the dominant social constituency's attempts to socially shape computing away from the hacker ethic.

Chapter 8 - Conclusion

8.1 INTRODUCTION - THEMES OF THE STUDY

8.2 CONTRIBUTION TO HACKING LITERATURE AND METHODOLOGICAL NOVELTY

8.3 SUMMARY OF FINDINGS - STATUS OF ORIGINAL RESEARCH QUESTIONS

8.4 CONTRIBUTION TO THEORETICAL KNOWLEDGE

8.5 UNANSWERED QUESTIONS - FUTURE RESEARCH

8.1 INTRODUCTION

This study is an empirical explanation of social theories of technological change and their emphasis upon the theme of closure. It describes attempts by the CSI and the dominant social constituency to stigmatise and marginalise hackers from any position of influence within computing. There is also a common call in social theories of technological change for a counter-cultural response to this process of perceived closure and the ethos of the dominant constituency. The form and rationale of such a culture is often left to speculation. This study investigates hacking as an actual representation of such a counter-culture.

To summarise briefly the progression of the closure argument in the study: the affinity hackers have with technology contrasts with the feelings of alienation the majority of people experience. The contrast gives rise to the initial respect given to hackers by the public who often perceive them as "computer whizz-kids", "technological wizards" and so on. More negative perceptions have arisen, however, especially within the CSI where there is a frequent failure to differentiate hackers from conventional computer criminals such as financial fraudsters. Hackers, in contrast, do differentiate amongst themselves, some claim to be representatives of "the hacker ethic" whilst denigrating others as unskilful "wannabes". This evolution and complexity of interpretation reflects the mix of motivational causes of the activity, combined with knowledge gaps within computing that complicate assessments of hacking's implications and potential worth. This lack of technical and ethical certainty gives rise to various shades of opinion as to the role and function of hackers. These shades of opinion are debated in the social process of closure.

This description of the process of "closure" is used as a means of addressing the major theoretical issues surrounding the subject of technological change, of which computer hacking is but one aspect. Chapter 3 introduced the concentration of the social shaping theorists

upon the need to develop a theoretical rejection of technological determinism. This study responds to that need by demonstrating how computer hacking is an illustration of the primacy of a social shaping-based explanation of technical change within computing over more determinist accounts. Latour's characterisation of technological change as the intrigues and machinations of "The Prince" identifies the most significant aspect of technological change as the question of the processes by which power is gained by one group and closed to others. The concept of the Prince is equated with the exercise of power. The dominant social order's power is best cemented through the use of technology. Technology, however, has ambivalent qualities, it represents both the site where power is manifested in physical form, but also where the purposes of that power are contested by groups such as hackers.

The study's analysis of closure within computing thus forcefully illustrates the double-edged nature of Latour's thesis. Technology cements social bonds that are already in place, but it can also be utilised by opposition groups to weaken them. The dominant constituency's desire to utilise technology to achieve this cementing of social bonds has been shown to require the increasing commodification of information. The study's examination of hackers' opposition to this commodification and their progressive exclusion from influence within computing is thus used as a specific illustration of Latour's Prince in action.

8.2 CONTRIBUTION TO HACKING LITERATURE AND METHODOLOGICAL NOVELTY

(i) Contribution to hacking literature

By highlighting both the complexity of the internalist account of hacking provided by hackers themselves, and some of the weaknesses of the externalist account of outsiders to the activity, the study serves to debunk some of the mythologising and hyperbole in the press's coverage of hacking, and provides a more well-informed

account. The importance of this study's contribution to work in the field resides in the dearth of material that attempts to evaluate seriously the views of hackers. Most of the existing material treats hacking tangentially, as in Turkle's Second Self, or concentrates upon the more sensational empirical aspects of hacking as in books such as The Cuckoo's Egg, Beating the System, Cyberpunk, and Approaching Zero.

The literature's tendency to report the sensational, concentrates upon hacking's negative aspects such as its tendencies towards obsessive and misogynistic behaviour, thus producing a rather one-sided account of the activity. To some extent, the study reinforces these negative impressions of hacking with it's analysis of the roles played within the activity of gender and addiction. It also, however, shows that these negative aspects of hacking are only a part of the activity's importance and significance for computing. The analysis of the range of other factors that motivate hacking, provides a more balanced and multifaceted account with which to aid a truer understanding of the phenomenon. For example, the evidence given in Chapters 4 and 5 combines to illustrate how hackers' technological curiosity has a potentially useful role to play in improving security standards within computing, and that this positive implication of hacking's technical knowledge is worthy of consideration along with its more negative aspects.

With the exception of Kane (1989) and Denning (1990), little attention has been paid by non-hackers to the non-addictive aspects of hacking. Writers tend to use evidence of obsessive computer use as proof of technological determinist fears that human values are jeopardised by the inexorable encroachment of machines, as illustrated by Weizenbaum's (1976) conclusion from his analysis of the effect of computers on the value placed upon human reason, that computers were the invention of the devil. Also, whilst the extant literature is agreed on the almost total predominance of men in hacking, very little has been written regarding the possible reasons for this situation. The study has sought to remedy this lacuna. The reasons for the male predominance of hacking seems to be

ambivalent, the situation seems due to a mixture of both the positive male penchant for technical problem-solving and the negative contributory factor of misplaced sexual inadequacy.

(ii) Methodological novelty

The study's novel methodological utilisation of e-mail correspondence, to supplement conventional interviews, is a direct response to the challenge of adapting the social scientist's methodology to "the network quality of the Prince's moves". (Latour 1986: 22) The study has utilised the medium of Computer Mediated Communication (CMC) as part of its exploration of the social processes behind technological change. It's use has made possible a more thorough investigation of the "gossamer framework" of the community and culture of hackers than would be possible by more conventional means. An example of this is the anonymous qualities of e-mail, described in Chapter 2. They enabled information to be extracted from hackers who would otherwise have been unlikely to risk communicating in a less secretive manner, for fear of prosecution. The use of e-mail has thus facilitated a first-hand examination of the opposition provided by hacking culture to the dominant social order.

A main empirical novelty of the study is its contrasting use of internalist and externalist accounts of hacking. The internalist account is the first-hand evidence given by hackers as an explanation of their culture and what motivates them. The externalist account consists of the views and perceptions of computing's establishment: those that are at pains to assert their non-hacker status. It is only through the contrast and conflict of these two accounts that the process of closure and transformation can be adequately analysed. Previous accounts of hacking have suffered from being rooted solely in either an internalist or externalist approach. This limits an analysis of the evolution of computer security as an issue to an essentially one-sided and static account that fails to appreciate the boundary-forming process

whereby the identities of both the CSI and CU are dependent upon the existence of each other. Specific aspects of this study that are empirically novel or substantial improvements on existing work are its detailed analysis of: the motivational characteristics of hacking; the reasons why hacking is overwhelmingly dominated by men; and the use of physical analogies in the ethical debate over informational property issues.

8.3 SUMMARY OF FINDINGS - STATUS OF ORIGINAL RESEARCH QUESTIONS

(i) Hackers and technological determinism

The study's description of the differing perceptions hackers and non-hackers have regarding hacking is of crucial importance for the exploration of its two main themes relating to technological control: first, the complex process whereby groups within society negotiate over the right to influence technology for their own purposes; and second, hacking as a particular illustration of the increasingly close nature of human interaction with technological artefacts. The study demonstrates the extent to which the gains and losses from IT are indeterminate and "up for grabs". Proving that an area of negotiability exists, helps to refute notions of technological determinism and contribute to its replacement with a more sophisticated account that describes how computing is socially shaped.

One of the initial questions of the study was whether the concept of technological determinism had relevance to the experiences of both the individual and the group as they seek to utilise technology. The account provided by hackers addresses the relationship of individuals to technology by the way it portrays their inventive curiosity. They are characterised by their ability to subordinate technology to their wishes rather than suffering the often prevalent feeling of being controlled by it. The account of non-hackers places more emphasis upon hackers' more "nerdish" and

addictive behaviour. In contrast to the hackers' own account, non-hackers perceive them as worshipping a 'silicon idol', having lost their humanity in a Faustian bargain whereby they become psychologically immersed in the machine.

The second technological theme regarding the way in which groups attempt to shape technologies is also illustrated by the differences between the two accounts. Extending its concern about people being able to control technology, the internalist account describes how the potential to socially shape computing has been lost due to the establishment's "construction of irreversibility". This is the process of closure by means of which hackers have mutated from their earliest days as pioneers of technological development to their present marginalised status on the fringes of computing. Whilst always having been idiosyncratic "outsiders" they have travelled from their early position inside the computer laboratory's of MIT to the "blustery Dutch field"[1] of the 1993 Hack-Tic computer club's summer conference.

The externalist account, in contrast to emphasising control of technology, explicitly admits that society's inability to technically secure its computer systems in the face of increasing levels of technological complexity has led to a need to stigmatise hackers. The baroque complexity of computing has produced a need to produce a social fix for a technological problem. In the words of Mr Arbuthnot MP quoted in Chapter 7: "There may be level of complexity in our society beyond which, because of safety interests we may be frightened to go. If hacking increases our fears ... that is a perfectly good and sufficient justification for the Bill." The failure of the externalist account to recognise the merits of aspects of the internalist account, whether this is deliberate or not, is thus compounded by technical pressures to exacerbate, not mitigate, the stigmatisation process. Increased levels of stigmatisation will, it is hoped, help to reduce the incidence of hacking and thereby lessen

---

[1] as described by Rupert Godwins, The Independent Friday 13th Aug 1993.

the need for increased technical measures to combat security weaknesses.

(ii) Hackers counter-culture status - internalist vs externalist accounts

Academic authors and the media have overwhelmingly concentrated upon the negative aspects of the motivations lying behind hacking. They have emphasised its addictive, "power-hungry" aspects, in addition to linking its prevalence with the purported sexual inadequacies of its adolescent practitioners. Chapter 4's analysis has shown that other motivating factors are also worthy of investigation, and this study's attention to the hackers' own accounts has illustrated the complex and mutually antagonistic mixture of several of these factors. Thus, for example, whilst the activity may involve some addictive attributes, this is only of limited importance in any overall explanation of hacking. Turkle's depiction of people sometimes using computers for psychological reasons of dependence or insecurity may indeed give an accurate description of compulsive programmers such as Paul Bedworth. However, as a full explanation and frame of reference for the type of hacking that is encountered in this study, it is lacking. The exact mix of hacking's motivating factors is complex and difficult to disentangle completely. This makes the issue of gender and why it should effect a person's proclivity to hack, for example, hard to evaluate conclusively. The difficulty is exacerbated by the fact that the internalist account has produced ambivalent evidence. The limitations of the 'nerdish' image portrayed in externalist accounts is challenged by the fieldwork evidence of the more positive intellectual, and potentially useful, aspects of hacking. Yet the image is also reinforced by the hackers use of language that incorporates addictive and sexual imagery.

The study thus provides a full-blown account of a group offering, at least an attempt to create, an alternative to the technological status quo. Criticism of that status quo riddles

technological writings. Theorists from differing schools of thought join in their calls for more human-orientated technology in various forms: "convivial tools" (Ivan Ilyich); and end to "one dimensional man" (Marcuse 1964); "technological politics" (Winner 1977); an "alternative social constituency" (Molina 1989) or "technical democracy" (Latour 1986). The study provides an original account of a group accepting Latour's warning not to hand technological superiority to the Prince on "a golden plate" by unquestioningly accepting its imposition (Latour 1986:24).

The opposition provided by hackers, however, is not without weaknesses. The potential of hacking to produce "the more humane" technologies normally associated with alternative cultures is possibly reduced by its tendency to encourage misogenystic behaviour containing elements of misplaced masculinity and/or sexual inadequacies. The gender and addiction-based critiques of hacking combine in Donna Haraway's notion of women embracing "cyborg power relations". Hackers represent a role model for counter-cultural recognition of the need to contest social power in full knowledge of its technological context. Haraway's feminist technological agenda acknowledges this, whilst seeking at the same time, to maintain recognition of the ultimate difference between the human body and the technology it is interacting with. She seeks to avoid the particularly male addictive willingness to totally embrace technology. Such willingness is shown by hackers who seek to "lose themselves" in their computer systems, thus Chip Tango "attaches his consciousness" to, or "butterflies around", a system. The gender-based criticism of hacking culture, however, may be mitigated by the possibilities CMC offers for non-gender-specific interactions between its users, as illustrated by "The Strange Case of the Electronic Lover" (cited in Dunlop and Kling [eds] 1992).

The charge that hacking represents more of an "alienated shopping culture" than a radical political group, received resonance in the fieldwork from some hackers' complaints that their main motivating factor is a lack of legitimate access, rather than the motivation of a coherent set of oppositional beliefs. The study's

evidence of hacking's obsessive traits also reinforces somewhat the belief that hacking's counter-cultural claims are weakened to the extent it represents domination by technology. The evidence is limited because the "visceral" association hackers make with technology can be equivocally interpreted as proof of their depth of their control over it or alternatively as subjugation to it.

Ross (1990) has been shown to criticise the cyberpunk celebration of the "aesthetic of detritus" which he argues leads to the danger of overstating the counter-cultural status of cyberpunks (and by extension hackers) as part of an "urban fantasy" fashioned more from white male middle-class fears of the "mean streets" than being based on any aspect of reality. The irony of this criticism lies in the fact that the criminalisation of hacking promoted by the authorities themselves,has hastened hacking's aura of "street credibility" and the aesthetic of detritus. They have done this by pushing it further towards the criminal fraternity than would have been likely if hacking had been left to evolve on its own steam. The fieldwork recounted, for example, John Draper's experiences in prison.

Despite the above weaknesses of hacking's status as an embodiment of alternative cultural values, positive oppositional qualities have been identified throughout the study. Hackers exhibit in the heterogenous range of their technological curiosity a celebration of human ingenuity's ability to subvert and manipulate a diverse stock of artefacts. This subversion is seen in acts, potentially disruptive to the social order, that range from the study's example of a Dutch hacker obtaining free time out of a parking meter, to the bringing to a standstill of the Internet communication system, which occurred as a result of Robert Morris Jr's worm program.

The nature of the CMC environment within which hackers operate has made identification of their oppositional potential difficult to establish, their anonymity producing a "gossamer culture". The intangibility of the culture has ambivalent implications for the researcher. On the one hand, the anonymity afforded by CMC enables relatively easy contact with hackers, but on the other hand, hacking's ability to effect computing and society from within has

been diminished by the process of closure, and as and its alternative status remains firmly rooted "underground", observation of its counter-cultural qualities is thus, on occasion, problematic.

(iii) Boundary formation

The origin of hackers' gradual lessening of influence within computing was described in Chapter 5's analysis of the software crisis, and the pressures it produced for a more scientific, as opposed to a craft-based, hacker-type, approach to software development. The main vehicle for the articulation of this process has been the use of physical analogies in the expression of particular ethical positions. This is an extension of the ethical debate, the origins of which are addressed in Chapters 3 and 4. Novel concepts such as cyberspace, initially presented in popular science-fiction, have been increasingly recognised as explanatory tools that can be utilised in understanding the implications computing's development has for the nature of information. The use of analagous thought upon which the new concepts are based is extended into the terms used in the ethical debate over the new issue concepts like cyberspace give rise to. The need of the dominant social constituency to use analogies in order to reevaluate ethical norms in their favour, is an important part of the closure process identified by this study, but otherwise ignored in the literature of computer security issues.

Latour's theory of the Prince contains the description of technological change as a scrabble-like game where competing groups use different strategies and ethical approaches in order to mould technology to their preferred shape. Some justification for such a view is contained in the evidence this study has provided from Chapters 5 and 6 that the CSI and CU have similar knowledge, but what differentiates them into separate groups (culture versus counter-culture) are the particular ways in which that knowledge is used. This implies that the subsequent dominance of one group over another is likely to be due to the success of one cultural outlook imposing itself on another. In this scenario, the marginalisation of

the CU away from mainstream influence in computing is due to a deliberate project of exclusion rather than any intrinsic inadequacy in the technical ability of, or potential benefits to be derived from, hackers and their knowledge. An example of such a project is the CSI and establishment's impugning or "smearing" of hackers' motivations. This is illustrated in both Chapter 6's section describing the CSI's strength of hawkish feeling and in Chapter 7's account of MPs discussing hackers in terms similar to those previously identified as part of a degradation ritual.

The use of analogies in the process of closure has been shown in Chapter 7's analysis of the passage of the Computer Misuse Act, and underlines hackers' arguments that criminalisation of their activity is a misdirected social response to the technical problem of insecure systems. The significance of the study's analysis of analogies is the way it shows the process of boundary formation taking place at the expense of technical solutions. The legislation is both a reflection of, and an exacerbating factor in, this process.

(iv) Stigmatisation

In order to show that hacking has been subjected to a deliberate process of stigmatisation, the research has thus described how in the nascent environment of computing, potentially useful information has been ignored or avoided for non-technical reasons. The rationales used are couched in terms of ethical and moralistic language that form part of a boundary-forming professionalisation process within computing. The stigmatisation process grows out of the fact that the changing nature of information threatens the dominant group's ability to control information specifically for its own ends. Hackers are a direct threat to the establishment's ability to enforce informational property rights, a threat exacerbated by technical tendencies which threaten the commodity status of information. Stigmatisation of hackers is used as a way of reducing their influence, and subsequently their threat, by marginalising them away from a position of influence within computing.

The stigmatisation project as the part of the boundary forming exercise is facilitated by the use of physical analogies. Chapter 5 illustrates, with admissions from CSI figures themselves, that it is difficult to find examples of intrusions achieved by particularly difficult means. This apparent ease with which computer intrusions occur means that victims of a computer intrusion may often feel more responsible and guilty than would the victim of a physical crime. Computer intruders are then compared to real world burglars so that they can be more readily associated with people who pose a criminal threat and physical danger rather than being associated with the relative benignity of mere intellectual hobbyists. They are thus used by victims of security breaches in order to more effectively condemn the perpetrators, in a process described by Herschberg in Chapter 5 as "blame displacement". It is a means of avoiding the culpability associated with lax security.

However, this blame-displacement exercise may not be smooth-running. It is, ironically, used in the first place to make up for the fact that computer intrusions are not particularly comparable to those of the real world. The ease of access to computer systems combined with a lack of physical threat or violence posed by hackers undermines the applicability of breaking and entering analogies to their activity. The fact that computer intrusions are more often associated with lax security than their real world counterparts, where some physical violence is normally required to overcome the physical security precautions in place, means that an immediate response to the victim is likely to be blame for inadequate security procedures rather than sympathy that the incident occurred.

The stigmatisation process, is part of the wider closure process by which the establishment uses technology to more effectively gain power. The study shows how the oppositional activities of hackers mean that the CSI and establishment groups do not have a free hand in exerting their influence over computing. Their need to stigmatise and implement closure in the first place is indicative of the complex process of defining different groups' status within computing, by means of negotiation and conflict. The example given of the

Bedworth case is a vivid illustration of the unresolved nature of the conflict. The polarised rhetorical ploys used in this legal attempt to deter hacking proved to be an inadequate method of dealing with the complex issues raised by it. They assumed a level of shared values between juries and prosecutors that may not in fact exist.

(v) Policy implications

Contrasting the internalist and externalist accounts shows the latter to be at least partially lacking, and this has direct policy implications for those attempting to establish a coherent institutional response to hacking. For example, there are mixed and inconclusive views as to whether increased access to, and education about, computing facilities may lessen or exacerbate the incidence of hacking. The motivations lying behind hacking are important to the success of legislation aimed at reducing the problem: legislation is likely to remain at the symbolic level if it is drafted in general ignorance of the phenomenon it is seeking to control. The strength and importance of curiosity as a motivation for hacking has shown the likelihood that hacking is a perennial human quality, only one aspect of which is its application to computers. The particular significance of hacking, however, rests with the increased social implications it has compared with other forms of technological curiosity, its higher profile is due to the centrality of computers in modern society.

Those aspects of the study that emphasise hacking's basis in technical curiosity imply that legislation aimed at detering it is unlikely to be very successful. Apart from the limited impact legislation is likely to have on peoples' innate curiosity, the unusually anonymous and fluid nature of hacking culture described in Chapter 4 also makes conventional punitive approaches difficult to enforce for the obvious reason that the perpetrators of hacks are difficult to identify. The inherent difficulties of successfully applying legislation to hacking gives rise to the charge that it is symbolic legislation. The establishment's desire to be seen to be taking action in response to

hacking appears to be more important than the likelihood of the response achieving its declared aims. Hackers are therefore more stigmatised than actively prosecuted.

8.4 CONTRIBUTION TO THEORETICAL KNOWLEDGE

This study compensates for the fact that the non-academic literature's approach to hacking has left little room for analysis of its larger theoretical issues. It covers those theoretical issues with an analysis of the significant characteristics of hacking that make it an identifiable culture actively involved in the development of computing, and thereby contributes to the social shaping debate of technological change. Hitherto these theories have tended to concentrate upon groups shaping technology from within the dominant constituency. Whilst the first hackers may have initially fitted this scenario, the study has described how successive generations of hackers have increasingly sought to influence computing's development from the outside, thus providing a novel perspective: oppositional influence within technological change. The emergence of the CSI, and the passing of the Computer Misuse Act, is evidence that this influence has not been insignificant.

Hackers represent an aspect of technological change that is not adequately covered in social shaping theories. Molina, along with Pinch and Bijker, for example, talk in terms of "sociotechnical constituencies" or "relevant social groups" which are instrumental in the development of a technology. They presuppose, however, an overall constituency with a generally agreed direction towards which the smaller groups within the constituency are aiming. Pinch and Bijker's, for example, utilise the notion of micro-social groups in their social construction of technology approach, which requires that assumptions about what constitutes a relevant group are easy to make. This study throws doubt upon their pluralist model by using the example of hackers to provide evidence of how counter-constituencies can arise within a technology. Pluralist accounts do not adequately take into account the issue of dominance, and how

relevant and non-relevant groups achieve and maintain their status. They tend to gloss over the fact that technological development may occur as a process whereby one group prevails over another resistant group with a fundamentally different value structure. In contrast, the particular case of hackers, demonstrates how counter-constituencies arise from such resistance. The study thus provides a fuller account of the concept of power by using hackers as an example of the struggle and contesting of power that occurs before it can be exercised in the process of technological change.

In response to technologically deterministic theories, social shaping analyses of the IT revolution strive to stem a tide of technological determinist pessimism. Such pessimism is also evident, however, even in otherwise optimistic social shaping approaches that look for areas within technology of potential political change that will reinforce the influence of the democratic 'social' over the technical. An example of this is Molina (1989) who shares with Mumford (1970) the conclusion that a more politically liberated form of technological development will only be achieved at the cost of, and by means of, a "catastrophe" whereby a "wholesale conversion of people to a new way of life" is necessary: "If mankind is to escape its programmed self-extinction the God who saves us will not descend from the machine: he will rise up again in the human soul" (cited in Molina 1989: 180). Social shaping theorists such as Russell and Williams (1988) also acknowledge areas of technological irreversibility which point toward the possibility that human choice and social shaping may be a real force, but a real force that exists in a circumscribed arena of intervention due to macro-induced limitations. This study has examined the role of hacking both as an embodiment of the 'human soul' and in its attempts to expand the circumscribed arena.

Latour recommends that the researcher should sit, "just at the point where the contract is made, just where the forces are translated, and the difference between the technical and social is fought out, just where the irreversible becomes reversible ... There, only a tiny amount of energy is necessary to drag a maximum

amount of information about its growth from the newborn monster" (cited in Knorr-Cetina 1981: 301). This is what this study has attempted to do by using hackers and their interaction with the establishment as a specific example of the point at which the "difference between the technical and the social is fought out": that is, the struggle between the CSI and the CU over the establishment of closure within computing. Whilst Latour's analysis highlights the laboratory as a site for the struggle between the social and the technical, this study has shown how hackers contest technical change far from the laboratory where closure is most keenly felt. Thus, the main theoretical contribution of this research stems from its analysis of hacking's important implications for theories of technological change.

Despite its critique of social shaping theories, the study agrees with their conceptual rejection of technological determinism. Although the study's internalist account of hackers emphasises this rejection by illustrating hackers' ability to control and shape technology, hacking can also be viewed in a more technologically deterministic manner. Chapter 3's analysis of cyberpunk fiction provides vivid examples of some of the technological determinist fears that hacking gives rise to. The image of hackers as "surfers on a technological wave", epitomised in the literature by Chip Tango, implies that although hackers utilise technology for their own enjoyment they do not influence its ultimate direction and therefore do not fully escape a determinist experience of technology. Hackers are in the words previously quoted from Meyer "a conscious resistance to the domination of, but not the fact of, technological encroachment into all realms of our social existence" (Meyer and Thomas 1990: 7). This implies that hackers object to the form computing has taken in society, but that their desire to see it used differently is still subordinate to their passive acceptance of its inevitable encroachment. This assessment of hackers is reinforced by Chapter 5's description of hacking's origin in the programming's software crisis. The fact that the best programmers and hackers are described as wizards, relates to the perception felt by predominantly

non-technical people that the technology they are manipulating constitutes a "black box" surrounded by an aura of "mystery" that even the hackers and programmers do not fully understand.

The dominant social constituency too, is not immune to perceptions of technological determinism in the sense that it has needed to react to the threat computing's technical development has posed to informational property rights. The adoption of physical analogies to develop new concepts is part of this attempt to deal with these changing technical conditions. Thus the technical induces a response from the social which would seem to be more in keeping with technologically determinist rather than social-shaping perceptions; it is an example of the "cultural-lag" thesis of technological determinism whereby societal institutions react to, rather than control, technical change. In this scenario the establishment, although overseeing the diffusion of computing, is itself struggling to come to terms with its social implications. It too, is faced with responding to the qualitatively new social situations which computing repeatedly produces.

The study, however, provides a rebuttal of temptations to interpret this scenario as society deterministically responding to the impact of technology. The struggle over the nature of computing, and by extension, information, fought between hackers and the dominant social constituency can be viewed as the price the establishment pays for using computing to increase its level of control in society. Theorists such as Latour (1986) describe this process in terms of a deliberate policy whereby the dominant social constituency encourages perceptions within society which hold that humans are largely unable to effect "autonomous" technological change (Chapter 3's concepts of inertia and automatism).

Diffusion of technology throughout society offers greater potential for increasing the establishment's power because it broadens the scope for implementing higher levels of inertia and automatism. The possibility of greater power has to be enforced to become reality, however, and it is in the conflict of competing strategies that hackers' status as a repository for alternative cultural

values lies. Hackers threaten the power-enhancing project of dominant social groups, and as a result, the strategies adopted by the establishment assume the qualities of Latour's Prince-like intrigues. An example of this is the establishment's stigmatisation of hackers. The externalist account depicts them as "nerdish" obsessives and our empathy with them is further eroded when they are portrayed as threatening our increasingly networked and safety-critical computer systems.

Hackers are an intrinsically interesting group at the forefront of issues connected with technological change because their activity described throughout this study opposes the strategies of the dominant social constituency. They oppose responses of inertia to technology with their manipulative and imaginative reinterpretation of uses for artefacts; they oppose automatism by calling attention to the political implications of governmental use of computing, and through their anti-bureaucratic ethos. The various limitations of hacking as an alternative cultural force, however, make it difficult to argue that hackers are likely to achieve any of their political aims, even presupposing that they have a coherently articulated and widely-shared program of action. This does not mean that hackers are redundant as a force of opposition, however. The inherent contradiction faced by the dominant social constituency's attempts to utilise technology to increase its own power is that the potential uses of that technology are double-edged: the technology's power is potentially available to both the dominant constituency and the counter-cultures seeking to oppose it.

Thus the research has provided evidence that hacking represents a significant site for those seeking to redefine society's development and implementation of technology. It opposes attempts to use technology to impose control without resorting to any form of Luddism. Instead, it utilises the very knowledge and artefacts used by the dominant social order to exclude groups with alternative agendas for technology. Instead of capitulating to the realities of existing social power by calling hopefully for an alternative technological ethos, hackers pursue democracy within the very

science and techniques that are being used against them. The disadvantage of this approach is that it risks becoming one with what it seeks to oppose. This is a charge made against hackers described by Ross (1990) in Chapter 3. Hackers are seen as the ultimate embodiment of establishment values for the way they exhibit "qualities that are valorised by the entrepreneurial codes of silicon futurism". The advantage of the hackers' approach, in contrast, is that it avoids the political fatalism and quietism of those like Marcuse and the Frankfurt School whose ultimate raison d'être became the avoidance of instrumental rationality in any form.

8.5 UNANSWERED QUESTIONS - FUTURE RESEARCH

This investigation ends with the fourth generation of hackers which contains both the "wannabe's" who reject the original hacker ethic and are involved in hacking for personal gain, and also the remaining "ethical hackers" who hack solely to satisfy intellectual curiosity. The impact of the establishment's response to this latest generation of hackers is still being felt, and it is likely that the conflict between the CU and the CSI will produce a fifth generation of hackers. This latest generation will occur as a result of the interaction between different constituencies. Future research might fruitfully examine, in retrospect, the impact of those aspects of the establishment's response to hacking such as The Computer Misuse Act. Because of the secrecy within the computing community engendered by the Act, the research has not been able to fully evaluate such questions as whether it has been effective in deterring hacking. Fuller access to such sensitive but potentially interesting areas as the banking sector and its contribution to the debate over hacking also proved largely unobtainable.

Finally, because of the wealth of social aspects that have stemmed from this analysis, less attention than desired was paid to the more specifically technical areas of hacking and some of the internal debates occurring within computing. The study has described those internal debates, such as the arguments over the

pros and cons of craft versus science-based approaches to programming, and the issue of the software crisis. The fact that these disputes exist at all, reflects how practices have not kept pace with the complexity of computing and this provides the space within which the hacker can operate. The ways in which attempts are made to resolve these debates in the future and the future implications of such developments as data encryption will have a decisive effect on whether hackers' technical knowledge and curiosity will still have a role to play in the social shaping of computing.

Appendix 1 - Statistical Analysis

1 QUANTITATIVE QUESTIONNAIRE RESPONSES
2 THE AGE FACTOR
3 POTENTIAL USEFULNESS OF BREACHES
4 STATE OF THE INDUSTRY

SECTION 1 QUANTITATIVE QUESTIONNAIRE RESPONSES

(N = 200)

Q1 Nationality

	Percent
US	53
UK	29
Europe	9
Australasia	4.5
Canada	3
Other	1.5
Total	100

Q2 Gender?

	Percent
Male	96.5
Female	3.5
Total	100

Q3 Age?

Age	Percent
15-20	4
21-30	52.5
31-40	24
40 +	19.5
Total	100

Q4 Organisation

	Percent
Academic	39.5
Commercial/manufacturing	12.5
Commerical R&D	19
Consultancy	7
Commercial services	2.5
Public services	2.5
Other	14
Combination	3
Total	100

Q.5 Computer security arrangements

	Percent
Too strict	1
Adequate	66.5
Lax	25.5
Combination	6
No comment	1
Total	100

Q.6 Formal qualifications in computing

	Percent
BSc	28
MSc	13.5
PhD	7
Other	41.5
Total	100

Q7 Incident experience

	Percent
All	22.5
Browse and hack	4.5
Malicious hack	6
Harmless browse	12
Virus	18.5
None	17
Virus and hack	7
Virus and browse	12.5
Total	100

Q8 Number of incidents

	Percent
10 +	19.5
None	17
1-5	50.5
6-10	13
Total	100

Q9 Severity of incident

	Percent
Very	6
Not Very	36
Not at All	28.5
Varies	12.5
Not Applicable	17
Total	100

Q10 Computing industry's concern with security breaches

	Percent
excessive	11
hysterical	12
combination	13.5
about right	37.5
insufficient	26
Total	100

Q11 Computer hacking as a crime?

	Percent
yes	52
no	25.5
don't know	22.5
Total	100

Q12 Satisfied with current legislation

	Percent
no comment	1
yes	12.5
no, too draconian	27.5
no, too weak	18.5
don't know	40
varies	0.5
Total	100

Q13 Adequate professionalism in the computer industry?

	Percent
no	33
don't know	30
yes	37
Total	100

Q14 Greatest threat to security

	Percent
insider	64
outsider	7.5
same	25.5
don't know	3
Total	100

Q15 Potential uses for viruses

	Percent
yes	40.5
no	31.5
don't know	28
Total	100

Q16 Potential uses of system breaking

	Percent
don't know	9.5
yes	67
no	23.5
Total	100.0

Q17 Future level of security breaches

	Percent
don't know	0.5
increase	73
decrease	7
stay the same	19.5
Total	100.0

Q18 Length of professional experience in computing

	Percent
1-5 years	31
6-10	27.5
11-15	18.5
16-20	20.5
0	2.5
Total	100.0

SECTION 1 SUMMARY:

The above responses to the quantitative questionnaire reinforce several points encountered in the qualitative fieldwork. Most notably, the extremely small percentage of female respondents is indicative of the low level of female participation in the areas of

computer security. In addition there are the following pertinent points to be made from the above responses:

Question 5: The evidence from the qualitative fieldwork seemed to emphasise the perceived widespread weaknesses of computer systems. In this particular response only 25% of people felt their systems to be inadequately secured. This may be explained, however, by the tendency of people to underestimate the weaknesses of the systems that they are associated with.

Question 6: The fact that much computing work is carried out by people without formal qualifications (41.5% of respondents) was mentioned in the main body of this study. This can be seen as due to both a lack of adequate levels of education in the computing industry, but also illustrative of the value of computing knowledge derived from practical hands-on experience rather than formal training.

Question 7: Only 17% of respondents had no experience of some kind of security breach. The experience of the different types of security breaches can be simplified as:

Malicious Hack or Browse	64.5%
Virus Only	18.5%
Nothing	17%

Question 14: 64% of respondents thought that insiders within an organisation posed more of a risk to its security than outsiders, whilst only 7.5% thought the converse.

Questions 15 and 16: The number of respondents who thought viruses and system breaking could be potentially useful was high. 40.5% and 67% respectively.

Question 17: 73% of respondents thought that the number of security breaches would increase in the future, compared with only 7% who thought they would decrease.

Figures 4a-c show how both academic and commerical organisations experience hacking to a similar extent (62 and 63% respectively), although the academic sector is almost twice as likely to experience viruses. In general there is quite a high level of security breaches with 25% of the academic sector experiencing all types of breaches and the commercial sector18%. The data for those experiencing no breaches is correspondingly low: academic sector 10%; commercial sector 25%.

The data also shows that both the academic and commercial sectors did not view hacking or viruses as particularly serious threats (6% and 7% respectively in figures 4d and 4e). Hacks and viruses are perceived as constituting a similar level of threat, 9% of hacks/browses being thought to be serious and 7% of viruses (figures 4f and 4g). There are relatively high and comparable figures for the number of repeated breaches of both hacks/browses and viruses. 17.5% of hacks and 16.5% of viruses had been experienced more than 10 times (figures 4h and 4i). Finally, as a reflection of the perception that breaches are not a serious threat figures 4f-k show how 66% of both academic and commercial sectors think that their security is adequate.

SECTION 2 THE AGE FACTOR
Fig.2a

Q3 What is your age?

	Percent
15-20	4
21-30	52.5
31-40	24
40 +	19.5

Total	100

Fig.2b

Age-group	Yes	No
15-20	12.5%	62.5%
21-30	50.5%	28%
31-40	60.5%	19%
40+	54%	20.5%

Section 2: Summary

The prediction of Chapter 6 that age would tend to encourage firmer ethical judgements is backed by the evidence from fig 2., although the over 40 age-group, whilst still adopting a more negative attitude to hacking than the youngest age-group are less liable to do so than the 31-40 group.

SECTION 3 POTENTIAL USEFULNESS OF BREACHES - Age and Organisational sector factors

Fig. 3a

Response by % of age group

Age Group	Yes	No	Don't Know	Row Total
15-20	62.5%	25%	12.5%	100%
21-30	75%	18%	7%	100%
31-40	67%	20.5%	12.5%	100%
40+	46%	41%	13%	100%

Fig. 3b

	Response		
	Yes	No	Don't Know
% of Organisational Sector			
Commercial	70%	21%	9%
Academic	63%	23%	14%
Other	69%	28%	3%

Section 3 Summary:

The fieldwork statistics show that significant percentages of the respondents believe that both hacking and viruses are of potential benefit. A view held across age groups with the 40+ group being less disposed to view either as useful. The belief that they are potentially useful is widely spread across organisational sectors.

SECTION 4.0 STATE OF THE INDUSTRY

The experience of security breaches by organisation type is summarised as follows:

Fig. 4b

	% of firms experiencing categories Hack/Browse	Virus	Nothing	All
Organisational Sector				
Academic	62%	70%	10%	25%
Commercial	63%	37%	25%	18%
Other	72%	51%	15%	26%

and:

Fig 4c.

% of total industry incidents experienced by organisational sector

	Type of Breach Hack/Browse	Virus	Nothing	All
Organisational Sector				
Academic	24.5%	27.5%	4%	10%
Commercial	26%	12.5%	10%	7.5%
Other	14%	7.5%	3%	5%

Fig. 4e

	Severity of incident as a % of organisational sector's incidents				
	very	not very	not at all	varies	N/A
Organisational Sector					
Academic	6%	46%	27%	11%	10%
Commercial	7%	24%	37%	9%	23%
Other	3%	41%	26%	13%	17%

Fig.4g

	Severity of incident			
Category	Very	Not very	Not at all	Varies
Hack/Browse	9%	44%	35%	12%
Virus	7%	43%	34%	16%
All	11%	33%	29%	27%

Fig. 4i

	Number of incidents of categories as a % of total incidents			
	0	1-5	6-10	10+
Type of incident				
Hack/Browse	35.5%	36%	11%	17.5%
Virus	42%	31.5%	10%	16.5%
All	77.5%	4%	5%	13.5%

Fig. 4k

View of security as a % of organisation type

Organisation Type	Too strict	Adequate	Lax	Varies	Don't Know
Academic	1%	66%	24%	8%	1%
Commercial	1%	66%	27%	5%	1%
Other	0%	69%	26%	5%	0%

Appendix 2 - Glossary of Terms and hacking case-studies

1. DEFINITIONS
2. THE GENERATIONS OF HACKERS
3. CASE-STUDIES

1. DEFINITIONS

The following defintions have been taken in large part from the electronic "underground" pulblication FBI, Volume 1 Issue 2.

Trasher Someone who searches, usually at night, the trash bins of companies for information that can help him/her make free/illegal use of phone or computer systems. It may even involve credit card numbers.

Crasher "This is a person who logs on to a system and causes it to crash, making it unavailable until the sysop [system operator] gets on and reboots the computer. These people can also access the databases and files of the systeme, making all of it available to himself."

Cracker A type of pirate who uses various, often ingenious, programming methods to break the copyright protection schemes on software that he and others may wish to use.

Computer Militant "This is a person who logs on to a bulletin bbs, or mainframe with the sole intention of destroying it and all it's data. These people have tremendous knowledge in the workings of a computer, but are generally less knowledgeable than a hacker. Many times these people are nothing more than disgruntled workers, or ex-workers who are enacting their revenge on the company."

Phreaker "This is a person who is very much like a hacker. Instead of attacking and learning about computers, he uses the phone lines as a toy. These people are generally equal to, or superior to most of the phone company itself in knowledge of the workings of a telephone service."

Rodent A "wanna-be" hacker who brags more than he actually accesses systems.

Code Kidz " This is one of the most hated people in the phreaker world. This is a person who acquires code to make long-distance calls, and does not give anything in return. He then proceeds to give the code to all his friends, and the code dies shortly thereafter."

Abuser An extreme form of a Code Kidz who incur extremely large calling bills with stolen phone-card numbers. "These people are hated by phreakers and the phone company alike. Neither abusers or code kidz have any knowledge of the phone system.

Donn Parker's description of "Crimoids"[1]

Donn Parker, an American computer security consultant defines a "crimoid" as an, "elegant, intellectually interesting method of computer abuse that receives extensive coverage in the news media...each crimoid illustrates the growing fragility of information in our society."

In addition to conventional hacking, his list of crimoids includes the following ...

i) Phone Phreaking

Illicit use of the phone system using imitation switching signals emitted by a "blue box" to achieve free use. First became known of in the 1970's and my research has shown it to be still occurring, one of my interviews being conducted by means of it of a prototype small touch-tone dialler which has come to replace the old, more cumbersome blue-boxes.

ii) Salami Fraud
A particular type of fraud relying on the automating of the debiting of small amounts of money from many accounts in large financial systems, made feasible only with the advent of the computer.

iii) Electronic Letter Bomb
A trojan horse attack that utilises a programming weakness in electronic mail messages. Discovered in 1979 by a group of anonymous students at the University of Berkeley California and publicised by a journalist in 1981.

---

[1] Denning P. (ed.) (1990) Computers under Attack pp 544-554 ed.

iv) Software Piracy
Illict copying of licensed software.

v) Radio Frequency Eavesdropping
The use of electronic equipment to pick up radio-frequency emanations and hence "listen-in" to the display screen of the computer under target.

vi) Interference
Taking over of a communication system and superimposing upon it your own message.

Two extra, potential crimoids of the future Parker mentions are:

* Voice mail terrorism- Attacks upon voice-mail systems within companies by phone-phreaks.

* Fax Graffitti- Saturation of company fax machines with obscene, pornographic or simply bothersome fax messages.

2. THE GENERATIONS OF HACKERS

The advent of hackers occurred with the computer pioneers of MIT described by Levy (1984).

The first generation - the "true hackers".

This first generation of hackers was responsible for the development of the earliest software. Hackers perceived themselves to be in opposition to a bureaucratic hierarchy that stifled their ingenuity. The earliest computers were large mainframe computers. Access to them was strictly controlled by laboratory technicians nicknamed 'the priesthood' by what came to be known in their turn as the 'mainframe' hackers. These hackers dedicated themselves, within the confines of MIT, to reducing the power of the 'priesthood[2]' and superseding it with the hacker ethic.

The second generation - the "hardware hackers".

This generation were known as the hardware hackers because of their major concern of liberalising access to computers from

---

[2] The phrase was used to describe the white-coated computer lab technicians that fed the early computers with the punch-cards containing the program instructions.

dependency upon mainframes through the mass dispersal of personal computers. Their expertise resided more significantly in the production of computer hardware than its software components. This project involved aspects of the 60's and 70's hippie movements. "Apple" Computers so derived its name, for example, because an apple was seen as a symbol of natural purity and wholesomeness. Freeing computing power so that it could be more widely available to society at large was viewed as a political act.

The third generation - the "Game Hackers".

Levy categorises this generation as a representation of the point at which "The Hacker Ethic had met the market place". (Levy 1984: 284). Within the third generation of hackers, such capitalist tendencies sat uneasily with their previous non-profit making ideal which emphasised the free flow of information devoid of proprietary claims. "The Third Generation lived with compromises in the Hacker ethic ... [they] never had the sense of community of their predecessors, and early on they came to see healthy sales figures as essential to becoming winners" (Levy 1984: 372).

As a result of this new found entrepreneurial spirit within hacking, those programs which did promise to produce large sales needed to be copy-protected. This led to the further compromising of the Hacker Ethic by some hackers themselves: "Oddly, most companies hired as copy-protection specialists the same kind of young hacker who commonly spent hours figuring out countermeasures to bust somebody else's protection routine." (Levy 1984: 374) This helped to produce the ambivalent situation whereby hackers were being employed to implement methods which endangered the Hacker Ethic.

3. CASE-STUDIES OF HACKING ACTIVITY

Maelstrom -case study of an American hacker

> I started out hacking on a local Michigan network which was then known as Merit Net. The first time I entered a system, the thrilling rush was better than the rush I get when finishing a program, so you can say I was hooked on the first try. Although I have never been caught phreaking, many of my friends have, so I made the natural transition to safer ways fo dialing out, such as using the PC-Persuit dialout modems directly accessible

through lymnet's network user addresses. I also scanned my local exchange and found a PBX I was able to use to hide my tracks when calling out, thus avoiding traces.

I learnt to use the Michigan C/NA (Customer Name and Address) bureau, which allowed me to dial up a computer and, after entering a passcode, use touch tones to get information on the owner of any Michigan telephone number. Some of my friends from around the world would start AT&T Alliance teleconferences every so often, and we would talk throughout the night, sometimes for as long as 12 hours at a shot (which was probably not good for grades at school). On one memorable conference Cellular Phantom demonstrated a REMOB number (REMote OBservation) which allowed us to listen in on any phone line in the country at will...I learned quite a bit about how much privacy people REALLY have as opposed to what they THINK they have.

In 1989 a local friend put up a world headquarters BBS for the West German group Red Sector Inc.. They were into writing Amiga demos, and were one of the top ten groups in the world, which got us a lot of interesting and well-known callers. We obtained a voice mailbox and put up a codeline on it, which was very popular for a long time. RSI made me an offer: if I would give them stolen AT&T calling card numbers to enable them to call the USA, they give me all the hardware I needed to have the ultimate computer system. I was offered computers, high speed modems, hard drives, and software...the only catch was their method. Using CBI or TRW's computer, some people use credit card numbers to steal merchandise, and by having stolen stuff sent to West Germany, they were able to escape detection when the theft was discovered since the post office there didn't keep records. This was against my morals, and I dropped out of the scene for a while.

Now I spend most of my time here at the college learning VMS on my legal accounts. I still have fun getting into computers on other campuses, but I don't really have the time I did before I started college. Many of my close friends have gone to jail or have quit the scene, so the inspiration to come up with neat hacks has also died down a little... (E-mail interview).

Trashing

> Personally, in those days, I would go through the wastebaskets in the Michigan State University computer centre. By comparing punched cards, I could scope out the username, account number and password. SMITH, AC5609, ROBBUE SMITG SMITH, AC5609, ROBBIW and so on, would allow me to go to a VDT and log on as Robbie Smith. From there, I would use help and try out the commands that sounded interesting. I even used my own real money later to pay for my access time. But I learned to use the Hustler Operating System created by MSU for their DCD6500 as a hacker. In the summer of 1990, my account at Lansing Community College was closed for hacking. I had tried the user/password routine on many accounts and found five or six inactive accounts this way. I used them to store textfiles such as library literature searches and so on. While my account was closed down, I used the "sense of the system" I had developed to continue working (E-mail interview).

Eric Coggans - aka - "Eric Bloodaxe"

All the hacking activity he refers to is in the past and he has had, and concluded, dealings with the U.S. Secret Service. This meant that he showed a willingness to discuss these issues not readily found elsewhere to the same level of direct experience:

> I have been active in the Computer Underground since approximately 1982. I have used the handle Erik Bloodaxe since that time. In 1984 I was asked to join a hacker group being formed called the Legion of Doom. This group would go on to become the most feared/respected/misunderstood entity in the history of the American computer underground. My own involvement with the Legion of Doom recently (March 1990) led to a raid of my home by the Secret Service. My desire as a hacker has always been to learn everything about every system so that in the future I could stand as one of the unquestionable experts in the field of computer security. I feel I am pretty damn close to that at this point. I plan on going into business in the near future as part of a computer security consultancy firm... **[This in fact happened in ..... and the firm is**

named ComSec, reference...] I have been in more systems than one can imagine, ranging from military installations, financial installations, to soda companies. I have seen insider-trading information, had access to transferrable funds, had the ability to manipulate credit information, and have had complete control over phone networks. Throughout my entire "career" as a hacker I have never used any system for personal gain of any kind, nor have I ever been the cause of any loss or destruction of data. I have never seen a virus, nor have I ever had one on any system I have owned...Hacking started out as mischievous curiosity. I wanted to see things that were hidden from my view. As I opened more doorways and became exposed to more and more information and the power that computers wield over everyday life I began to fall prey to the power that comes with the knowledge that once you control the computers you control the world. I outgrew that and now I basically hack because it is a habit that is incredibly hard to break. Much like a junkie in need of a fix, I find my self turning on the computer and digging around without even thinking. I've been hacking for half of my life. I challenge anyone to try to stop doing something that they have enjoyed for half of their life.

"Adlacy" - Irish hacker

I cracked an ICL 39 series level 80 running GMAC. It was a new computer in college with less security than a Unix. It was easy partly due to an admin thing of having a standard type of no. for passwords and also very much due to the way the OS (operating system) was set up. I ended up with many Megabytes of extra space, many class projects for the next four years of college and a warning never to do it again. I got caught for printing out all I had access to. It was rather large...it was stopped after a boxful of paper.

I didn't think college would take it so seriously. There was a threat of kicking me out of college (to scare me into never doing it again I'd imagine). I also had to pay for the box of paper. Funnily enough, I would'nt hack now. In fact I've been given many opportunities since, and haven't taken up on them.

Everyone else heard about it. They also heard that I might be kicked out of college, and that I got a summer job as a result of it.

References

Barlow, John Perry "Crime and Puzzlement", Whole Earth Review, Fall 1990, p. 44-57.

Bequai, August. (1987) Technocrimes, Lexington (Mass): Lexington, USA.

Bijker, Wiebe E., Hughes, Tom and Pinch, Trevor (eds.). (1987) The Social Construction of Technological Systems, MIT Press.

Bijker, Wiebe E., (1993) "Do not Despair: There is life after Constructivism" Science, Technololgy, & Human Values, Vol 18 No.1, Winter 1993, p. 113-138.

Bijker Wiebe E., and Law, John (eds). (1992) Shaping Technology/Building Society: Studies in Sociotechnical Change, MIT Press.

Bloombecker, Buck. (1990) Spectacular Computer Crimes, Ilinois USA, Dow Jones-Irwin.

Borden, Elizabeth. "Sexism and the CU" Computer Underground Digest, Vol. 3.00 file 4.

Bowcott, Owen and Hamilton, Sally. (1990) Beating the System, London, Bloomsbury.

Bowcott, Owen. "Hacking and the Bedworth Syndrome", The Guardian, (Review Section:19), Thursday, April 1, 1993.

Brady, Tim. (1988) "Crisis What Crisis?", Paper prepared for the PICT Software Workshop, UMIST 18-19 July 1988.

Brunner, John. (1969) The Shockwave Rider, New York: Ballantine.

Callon M. and Latour B. (1981) "Unscrewing the Big Leviathan: How Actors Macro-Structure Reality and How Sociologists Help Them Do It." In Knorr-Cetina K. and A. Cicourel (eds.) Advances in Social Theory and Methodology: Towards an Integration of Micro and Macro Sociologies, Routledge, London, p. 277-303.

Carr, Edward. "Elemental Issues", Micro Decision , June 1990, p. 30-31.

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

The Dark Adept. "The Hermetic Underground", Computer Underground Digest, Vol. 2.15, File 7 of 7.

De Lacy, Justine. "The Sexy Computer", in Computers in the Human Context, Forester, Tom (ed.). (1989) Basil Blackwell, Oxford.

Denning, Dorothy E. (1990) "Concerning Hackers Who Break into Computer Systems." Paper presented at the National Computer Security Conference, Washington, D.C., October 1-4 1990, p. 653-664.

Denning, Peter J. (ed). (1990) Computers Under Attack: Intruders, Worms and Viruses, ACM Press and Addison-Wesley.

Doctor Crash. (1986) "The Techno-Revolution", Phrack, 1 (6): Phile 3.

Dougan, William and Gieryn, Thomas. (1990), "Robert Morris: Worm? Virus? Hero?", Unpublished paper, Sociology Departments of UCLA and Indiana Universities.

Dunlop, Charles and Kling, Rob (eds.). (1992) Computerization and Controversy: Value Conflicts and Social Choices, Boston, Academic Press.

Elliot, Christopher and Mackay, Angela. (1993) "Everyone pays a high price to beat hackers", The Times, p. 5.

Forester, Tom and Morrison, Perry. (1990) Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing, MIT Press.

Gibson, William. (1984) Neuromancer, London, Grafton.

Gibson, William. (1986) Burning Chrome, London, Grafton.

Gibson, William. (1987) Count Zero, London, Grafton.

Gibson, William. (1988) Mona Lisa Overdrive, London, Grafton.

Gold, Steve. "Computer Security", Micro Decision, June 1990, p. 47-61.

Goldstein, Emmanuel. "Response to Telecom Digest's views Computer Underground Digest, Vol.1:13, July 1990.

Goldstein, Emmanuel. "Hacker testimony to House Subcommittee largely unheard", Computer Underground Digest, Vol 5:43.

Goodwins, Rupert. (1993) "Motley bunch hack at the end of universe", The Independent, Friday 13 August, p.11.

Haffner Kate, and Markoff John. (1991) Cyberpunk: Outlaws and Hackers on the Computer Frontier, London, Fourth Estate.

Hansard, Parliamentary Debates, Standing Committee C, Wednesday 28 March, 1990.

Hansard, Parliamentary Debates, House of Commons, 9th Feb, 1990.

Haraway, Donna. (1985) "A Manifesto for Cyborgs: Science, Technology, and Socialist Feminism in the 1980's", Socialist Review, no 80, p. 40-55.

Harris, Gillian. (1993) "Computer hacking 'addict' is cleared of conspiracy", The Scotsman, Thursday March 18, p. 1.

Harris, Gillian. (1993) "Daring data raider dependent on hacking fix", The Scotsman, Thursday 18 March, pg 3.

Holloway, John and Peláez, Eloina. "Learning to Bow: Post Fordism and Technological Determinism" Unpublished and undated paper, Edinburgh Unversity.

Hollinger, Richard C. and Lanza-Kaduce, Lonn. (1988) "The Process of Criminalization: The Case of Computer Crime Laws." Criminology, Vol 26, No.1, p. 101-126.

Independent editorial (1993) "Odd addiction, perverse verdict", Thursday March 18, p. 25.

Johnson, Bob. "What the Laws enforce" RISKS 11.32, March 1991.

Johnston, M. and Wood D. (1985) Right and Wrong in Public and Private Life, Gower, U.K.

Kane, Alan and Mason, John. (1993) "When hacking turns into an obsession", Financial Times, Thursday 18 March, p. 7.

Kane, Pamela. (1989) V.I.R.U.S. Protection: Vital Information Resources Under Siege, Bantam, New York.

Keller, Laurie S. (1988) "Machismo and the Hacker Mentality: Some personal observations and speculations". Paper presented to WiC (Women in Computing) Conference, p. 57-60.

Koestler, Arthur. (1967) The Ghost in the Machine, London, Hutchinson.

Landreth, Bill. (1985) Out of The Inner Circle, Washington, USA, Microsoft Press.

Latour, Bruno. (1986) "How to Write 'The Prince' For Machines As Well As For Machinations". Working Paper, Edinburgh University Seminar, June 1986.

Latour Bruno. (1981) "Give me a Laboratory and I Will Raise The World" in Knorr-Cetina K.D. and Mulkay M. (eds.), Science Observed, London, Sage, p. 293-321.

Laughlin, Chet. "What the Laws enforce Debate", RISKS 11.34, March 1991.

Levy, Stephen. (1984) Hackers: Heroes of the Computer Revolution, New York, Bantam Doubleday Dell.

Lundell, Allan. (1989) Virus! The Secret World of Computer Invaders that Breed and Destroy, Chicago, Contemporary Books.

Lynas, Mark. (1993) "Mother Tells of Hacker's Addiction", Edinbugh University Student Newspaper, p. 1.

MacKenzie, Donald and Wajcman J. (eds.). (1985) The Social Shaping of Technology, Milton Keynes, Open University Press.

Marcuse, Herbert. (1964) One-Dimensional Man: Studies in the Ideology of Advanced Industrial Society, Boston, Beacon Press.

Matthews, Dave "A Bug in the Machine" The Sunday Correspondent, 17th December 1989, p. 37-41.

The Mentor. "The Conscience of a Hacker" Phrack, Vol 1 Issue 7, phile 3 of 10.

Metcalfe, Stanley. (1986) New Electronic Information Services: An Overview of the U.K. Database Industry in an International Context, London, Aldershot Gower.

Meyer, Gordon R. (1989) "The Social Organisation of the Computer Underground", Unpublished Masters Thesis, Northern Illinois University.

Meyer Gordon R., and Thomas, Jim. (1989) "Baudy World of the Byte Bandit: a post-modernist interpretation of the CU", paper presented at the American Society of Criminology annual meetings, Reno, November 1989.

Meyer Gordon R. and Thomas, Jim. (1990) "(Witch)Hunting for the Computer Underground: Joe McCarthy in a Leisure Suit", The Critical Criminologist, 2nd September 1990, p. 225-253.

Michalowski, Raymond and Pfuhl, Edmund. "Technology, Property, and Law: The Case of Computer Crime", Contemporary Crisis, 1990, p. 250-283.

Molina, Alfonso. (1989) The Social Basis of the MicroElectronics Revolution, Edinburgh University Press.

Molina, Alfonso. (1989 a) The Transputer Constituency: Building up U.K./European Capabilities in Information Technology, Edinburgh University PICT Research Report Series No.1 1989.

Mungo, Paul. (1991) "Satanic Viruses", Gentlemen's Quarterly, Feb. 1991, Issue 20 (British Edition), p. 126-130.

Mumford, L. (1970) The Myth of the Machine: The Pentagon of Power, Harcourt Brace Jovanovich, New York.

Nuttall, Nick. (1993) "Healthy hobby that becomes obsession", The Times, Thursday March 18 1993, p. 5.

Parrish Jr., Edward. "Hacking is a crime, Pure and Simple", Phrack Vol 2, Iss 24, Feb 1989.

Peláez, Eloina. (1988) "A Gift from Pandora's Box: The Software Crisis" PhD Thesis, Edinburgh University.

Peláez, Eloina. (1990) "Soft Ware", Paper for the workshop on Social Perspectives of Software, Oxford, January 1990.

Phillips, Martin. (1993) "Computers Turned My Boy Into A Robot", Daily Mirror, Thursday March 18 1993, p. 1+4.

Pinch, Trevor and Bijker, Wiebe E. (1984) "The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other." Social Studies of Science, Vol.14, p. 399-441.

Pithers, Malcom and Watts, Susan. (1993) "Hacker penetrated MoD", The Independent, Tuesday 18 March 1993, p. 1.

Rasmussen, Bente and Hapnes, Tove. (1991) "Excluding Women From the Technologies of the Future? A case study of the culture of computer science", Futures, December 1991.

Ross, Andrew. (1991) Strange Weather, Verso.

Roszak, Theodore. (1986) The Cult of Information: The Folklore of Computers and the True Art of Thinking, Cambridge U.K., Lutterworth Press.

Russel, Stewart and Williams, Robin. (1988) Opening the Black Box and Closing it Behind You: On Micro-Sociology in the Social Analysis of Technology, Edinburgh University PICT Working Paper Series.

Saffo, Paul. (1989) "What is Cyberspace?" Communications of the ACM, Vol. 32, no.6 p. 664-665.

Schell, Roger R. (1979) "Computer Security: the Achilles' heel of the electronic Air Force?" Air University Review, January-February, Vol. XXX No.2 p. 16-33.

Shallis, Michael. (1984) The Silicon Idol: The Micro-revoloution and its Social Implications, U.K., Oxford University Press.

Shotton, Margaret A. (1989) Computer Addiction? A Study of Computer Dependency, London, Taylor and Francis.

Silicon Surfer. "Playgrounds of the Mind: Cyberspace", Computer Underground Digest, Vol. 2:17.

Spafford Eugene H. (1990) "Are Computer Hacker Break-Ins Ethical?" Purdue University Technical Report, CSD-TR-994.

Spafford Eugene H. (1991) "Three Letters On Computer Security and Society", Purdue University Technical Report, CSD-TR-91-088.

Spertus, Ellen. (1991) "Why are There so Few Female Computer Scientists?" Unpublished paper, MIT.

Stallman, Richard. (1985) "The GNU Manifesto", Cambridge, USA, Free Software Foundation.

Steele, Kate. (1988) "The Social Construction of the Software Crisis", unpublished work placement report, The Centre for Research into Innovation Culture and Technology, Brunel University.

Sterling, Bruce (ed.). (1988) Mirrorshades: The Cyberpunk anthology, London, Paladin.

Sterling, Bruce. (1993) The Hacker Crackdown, London, Viking.

Stockfield, Bob. (1991) "Why the Legion of Doom has little to fear from the Feds", Business Week , April 22, 1991, p. 62..

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

Thomas, Jim. (1990) "Review of the Cuckoo's Egg" CuD Vol 1.06, File 4 of 5.

Thomas, Jim. "EFF Response to the Atlanta sentencing", Vol. 2.07, Computer Underground Digest.

Thompson, Ken. (1984) "Reflections on Trusting Trust", Communications of the ACM, Vol 27, No.8., p. 761-763.

Toxic Shock Group. "The Evil That Hackers Do" Computer Underground Digest, Vol. 2.06: File 4 of 5.

Turkle, Sherry. (1984) The Second Self: Computers and the Human Spirit, London, Granada.

Uitenbrauer, F. "Computer Abuse Proposal Gives Police Lot of Room for Discretion" (translation of title), NRC Handelsbad (Amsterdam) 23 April, 1991.

Vallee, Jacques. (1984) The Network Revolution: Confessions of a Computer Scientist, London, Penguin Books.

Vinten, Gerald. (1990) "The Criminalisation of Hacking: A Boon To Computer Security?" Unpublished Paper, The City University Business School, London.

Watts, Susan. (1993) "Trial haunted by life in the twilight zone", The Times, Thursday March 18 1993, p. 4.

Weizenbaum, Joseph. (1976) Computer Power and Human Reason, San Francisco, Freeman.

Winner, Langdon. (1971) Autonomous Technology, MIT Press.

Woolgar, Steve and Russell, Geoff. (1990) "The Social Basis of Computer Viruses", Brunel University, CRICT Discussion Paper.

Zimbardo, Philip. "The Hacker Papers", Psychology Today, August 1980, p. 62-69.

ELECTRONIC MAGAZINE CITATIONS

Computer Underground Digest, Vols. 1-5: 1990-1993.

RISKS Digest, 1990-1993.

List of Interviews

Hackers - Face-to-face interviews

The Hack-Tic hackers (3 people)	Dutch Hacking-Magazine
Mike	Dutch hacker and phone-phreak
Ralph	Dutch Hacker
Graeme Rule	Ex-hacker, Edinburgh University Computing Officer
Robert Schifreen	The 'Prestel hacker', Managing Director of TKK Computer Security Ltd.
"The Zoetermeer Gang" (4 people)	Dutch University Hacking Group

Phone interview

Kevin Mitnick	"The Dark-side Hacker" from Cyberpunk

E-mail correspondence

Adlacy	Irish hacker
Altenkirch	German hacker

Eric Coggans	Ex- "Legion of Doom member"
Jean-Paul Condat	President of the French Computer Chaos Club
John Draper	"Captain Crunch" Phone Phreak and hacker
Faustus	German hacker
Martin Freiss	German hacker
Eric Hunt	Undergraduate in CIS at Birmingham-Southern College Alabama, USA
Maelstrom	USA hacker
Mercury	USA hacker
Mofo	USA hacker
Rob Nauta	Dutch hacker
Tester	USA hacker
Andy Vaught	Irish hacker
"Works Admin"	USA hacker

Academics - Face to face

Tim Bradshaw	Edinburgh University AI department
John Butler	Edinburgh University Computing Officer
Prof Hirschberg	Computer Science Professor Delft University, The Netherlands

Edwin Kremer and colleagues	Utrecht University Computer Science Staff
Rob McCron	Edinburgh University Computing Officer
Andie Ness	Edinburgh University AI department
Joseph Weizenbaum	MIT Computer Scientist and author

E-mail correspondence

Hylton Boothroyd	Warwick University
Prof Brunnstein	Hamburg University
Dr England	Glasgow University
Gerry Santoro	Computer Science professor Penn state university, USA
Prof Spafford	Purdue University, Indiana, USA
Brian Thompsett	Hull University Computer Science Lecturer
A. Turland	Edinburgh University
Warman	London Business School

Computer Security Industry -	Face to Face
Tony Elbra	National Computing Centre Security Division
Mr Van Gaalen	TSB National Computer Security Division, Wilmslow

Dr Taylor	Computer Security Consultant and Ex-chairman of the British Computer Security Commitee
Bernard Tozer	Computer Security Consultant and member of the British Computer Security Commitee
J. C. Van Winkle	Dutch Software Engineer

E-mail

Fred Cohen	Researcher and Creator of 1st documented virus
Sanford Sherizen	Computer Security Consultant and Author
	USA Programmer/Software engineer/System Manager
Barrie Bates	"
Bob Bickford	"
Btimberl	"
Carlson	"
Wayne Christopher	"
Bernie Cosell	"
Fred Davidson	"
Eric Donaldson	"
Forbush	"
Steve Hardin	"
Brendal Kehoe	"
Paul Kerchen	"
Lparks	"
Peter Da Silva	"
Rob Slade	"
Smb	"
Zmudsinki	"

Carapetis	Australian system manager
Daniel Cunliffe	Edinburgh Unversity programmer
Amos Shapir	Israeli programmer

Other interested parties

Face-to-Face

Michael Campbell	Tardis - "Time Lord"
Mike Jones	Security awareness division: DTI-London
Detective Harry Onderwater	Dutch Criminal Research Institute- The Hague
Mr Va de Pous	Dutch (Amsterdam) computer journalist

E-mail

John Perry Barlow	Co-founder of the Electronic Frontier Foundation, lyricist for the Grateful Dead
Krista Bradford	USA journalist (researcher for Geraldo programme)
Richard Stallman	President of the "Free Software Foundation
Clifford Stoll	Author of The Cuckoo's Egg

List of Abbreviations

A C M	Association for Computing Machinery
B C S S C	British Computer Society Security Committee
C M C	Computer Mediated Communciation
C S I	Computer Security Industry
C U	Computer Underground
C u D	Computer Underground Digest
I T	Information technology
N C C	National Computing Centre
N S A	National Security Agency