From Underground Hacking to Ethical Hacking

Donna Peacock

PhD

2013

From Underground Hacking to Ethical Hacking

Donna Peacock

A thesis submitted in partial fulfilment
of the requirements of the
University of Northumbria at Newcastle
for the degree of
Doctor of Philosophy

Research undertaken in the
School of Arts and Social Sciences

September 2013

Table of Contents

List of Tables

Abstract

This Thesis explores the nature and practice of ‘Ethical Hacking’. Ethical Hackers are individuals who use hacking skills, knowledge and techniques within legitimate authorised practice; they are employed to Hack.

A Critical Realist methodological approach is employed in order to gain a qualitative understanding of a real phenomenon through a range of key informants who provide personal narratives within semi-structured interviews, commenting upon their own realities, and their perceptions of the field in which they work.

A Bounded Rational Model of decision making reveals that decisions relating to involvement in criminality and individual Hacking events are made through a process of reasoning, of approximating the net gains and losses of a particular course of action, and that these decisions are ‘bounded’ by social norms, ethical approaches and the personal motivations and social circumstances within which the decisions and behaviour are framed.

Acknowledgements

I would like to thank Professor Michael Rowe for his supervision of this thesis, which has allowed me the flexibility and the freedom to grow and to develop into a researcher in my own way.

Thanks to Patrick Hutchinson for supporting me through the times when this project seemed too difficult to complete.

Thanks to Wendy Podd for your methodological insights, and to Stephen MacDonald for the theoretical debates which helped me to formulate my ideas.

Finally, I would like to thank the 23 people who were interviewed for this research for their time and their valuable insights into Ethical Hacking, whose contributions have been immeasurable.

Declaration

I declare that the work contained in this thesis has not been submitted for any other award and that it is all my own work. I also confirm that this work fully acknowledges opinions, ideas and contributions from the work of others.

Any ethical clearance for the research presented in this thesis has been approved. Approval has been sought and granted by the University Ethics Committee on 21/05/08

Name

Signature

Date

Chapter 1: Introduction

1.1 Introduction

This thesis examines those Hackers who use their skills legitimately as a source of income. It utilises a Critical Realist framework to focus upon the nature of crime, harm and wrong through the lenses of law, ethics, and morality in order to better understand the nature of what has come to be termed 'Ethical Hacking' and how it relates to traditional understandings of Hacking behaviour, and the reasons and motives which underlie it. A particular focus is the factors which lead to decisions about individual Hacking events, careers and desistance. A Bounded Rational Model (Simon, 1957; Clarke and Cornish, 1985; Cornish and Clarke, 1986; Gigerenzer and Selton, 2001; Selton, 2001; Cornish and Clarke, 2008) will be used to explain the nature of this decision making.

New technology has always generated fear in society (Kirkpatrick, 2004). This has been the case with many now taken for granted technologies. This societal fear has been associated with fear of change, and fear of the unknown (Mordini, 2007). Since the outset of computing, and more recently, the networking of computers, writers have exploited this fear in creating genres of literature including sci-fi and cyberpunk, which have defined these societal fears and have brought the terms Hacking and cyber-crime into the public consciousness. It has been suggested that this is related to the rate of technological change within late modernity:

> Modernity is confronted with revolutionary and accelerated changes in science and technology that challenge basic implicit and explicit moral assumptions and

> legal norms. This makes many people feel uneasy with technology, they wonder if it is safe, and they have trouble coping with constant change.
>
> (Mordini, 2007: 546)

Hacking itself began as a rather benign activity (Levy, 1984; Sterling, 1992) and has been sensationalised by the media (Kirkpatrick, 2004) along with other forms of cybercrime into a source of social anxiety (Pfuhl, 1987; Kane, 1989).

This has led to a number of attempts to regulate and legislate against cybercrime (see Chapters three and six), along with a dramatic alteration of the nature of understandings of Hacking, and a shift in the activities which are covered by the term (Taylor, 2000; Chiesa and Ducci, 2008).

There has been the emergence of a Hacking community which once regulated has split so that we now see two distinct groups; those Hackers who are ‘underground’ with affiliations to the traditional Hacking community and who have been quite extensively profiled, and those Hackers who have come to be co-opted or affiliated with the regulatory systems or powers but who nonetheless share the same skills, knowledge and experiences. As this study shows there is often an overlap between the two groups. There are shared activities and motivations, shared communities and networks; despite these commonalities the two groups are distinct from one another in the apparent desistence from crime of Ethical Hackers – this choice and the factors which inform it will be examined. Many of the respondents engaged in complete desistence, but often the Ethical Hacker persists in engaging in criminal behaviours and illicit knowledge sharing.

This chapter will introduce the research questions and will provide a brief discussion of how these were formulated. The chapter will outline the aims and objectives of the study, along with a description of how these will be met. The theoretical position, methodological approach, ethical issues arising and the findings of the research will also be briefly outlined. A concise overview of each of the remaining chapters will follow.

The aim of this research is to begin to theorise a new and emerging social entity, namely the ‘Ethical Hacker’. It is therefore of importance to those individuals working within the field, to employers within both the public and private sectors, and also to those who buy the service, either as organisations or as private individuals and to those who engage in education and training within the field. This research also has implications for the Criminal Justice System as a whole, and in particular for the judiciary who have a significant role as buyers of the service, as well as in controlling criminality.

This development to the Hacking world has not been fully examined within the current literature. This has necessitated an extensive and ongoing review of current knowledge, identification of gaps in the available literature and generation of data which can begin to fill these gaps.

1.2 The development of the Research Question

This study was commenced with a simple initial question which emerges from any review of the extant scholarly and academic writing on the subject which reveals that there are currently significant gaps in the knowledge which relates to Ethical Hackers. This has led to the development of the research question:

- **What are the decision making structures that inform the nature and behaviour of Ethical Hackers?**

As the review of the extant literature progressed, it became apparent that there has been some movement of individuals from the illicit Hacking which society fears, into the more acceptable face of Hacking which has now come to be termed as 'Ethical Hacking' by the academic community these 'Ethical Hackers' are employed to use their skills and knowledge in Hacking. Hackers therefore appear to be involved in the same activities and behaviours, and using the same skills and knowledge, but the purpose and the motivation has shifted. This research commenced with the aim of finding out why and how they make this choice. It may be that it can be linked to the desire to avoid prosecution and create a legitimate income because of life stage development, which means that as these Hackers age they come to be more likely to have real world relationships and responsibilities. It may be that those individuals who choose to engage with then legitimate face of hacking do so because they come to be more risk averse and choose to act legitimately rather than acting outside of the law. The fulfilment of these aims invites engagement with a range of criminological literature and theoretical debates relating to subcultures, deviance, desistance and social control. These are considered at greater length within Chapter Two.

Whilst there has been much discussion and debate about the personality and social characteristics Hackers and the nature of their social organisation and communities, the Hackers who have been studied in the past have generally been under the age of 30 (please see chapter two). What was unclear was why they should be, on average, so young. A range of possible suggestions emerges. It could be that as these Hackers age they begin to desist from Hacking, in which case it is of interest why and how this has occurred. It could be that they stop getting caught as they become more highly skilled, and therefore they are more anonymous and less accessible to the social researcher. This research aimed, at the outset, to consider those who apparently chose desistence from criminality.

In order to begin to address some of these issues semi-structured interviews have been conducted with legitimately employed Hackers, who use the same skills, knowledge and experience as traditional Hackers, but within their job role. The respondents have all, at some stage in their career, operationalised Hacking techniques for the purposes of security, or are currently doing so. The interviews began to reveal some interesting facts about this group of 'Ethical Hackers', but also suggested that the original assumptions were incomplete. As this study will show the Ethical Hacker is not only drawn from an illicit background, in fact many of the respondents claim that they have never acted illegally, and that they never would.

With the above frame of reference, this study commenced with the aims of finding out who these Ethical Hackers are as individuals and as a social group, specifically what it is that they do, and why they choose to do it. This includes an examination of the choices that they make about individual events, about ongoing choices and about careers, persistence, behaviours and affiliations. Within this is an examination of how they see themselves in relation to the Hacking and Ethical Hacking communities, the extent to which they engage with other Hackers, both ethical and underground, the structure of these groups, and the impact that this has upon decision making. Notions of right and wrong have been examined, particularly in relation to ethics, morality and legality and how these frameworks impact upon decisions about how to behave as will be explored in depth in Chapter Six.

A review of the available literature is suggestive of a number of areas for further research. Firstly, ‘Ethical Hackers’ as a social group have not been empirically examined in relation to their social relationships, or construction of status and identity. ‘Ethical Hacker’ culture and social organisation have not been examined, along with transformations in the status, identity, motivations and personal power. An exploration of the ‘Ethical Hacker’ may offer new insights into these issues. The development of the ‘Ethical Hacker’ and how this development shapes views and behaviour with relation to morality, ethics and the law have not been previously studied. The findings of this research must be considered within a context of how and why computing and cyberspace developed in the ways that they did, the new opportunities that these have created, and also the social reactions and anxieties which have shaped how society perceives Hackers, their activities, and their environment; this context is provided within Chapter Two.

The interviews carried out have attempted to address all of these issues and questions which are of interest to the research, but also to gain an understanding that is appreciative of the perspectives of the people involved.

1.3 Aim

On the basis of the developments outlined above, the research has been focused around one central aim:

> **To explore the phenomenon of ‘Ethical Hacking’, its emergence, its development and practice, and its relationship to more traditional understandings of Hacking as an activity.**

1.4 Objectives

Underpinning the broad aim of the study are the following objectives

- Examine the definitional difficulties around the nature of Hacking, and Ethical Hacking.
- Examine the role of academia, business and the security industry in the social construction of the ‘Ethical Hacker’.
- Explore the social behaviour and relationships of ‘Ethical Hackers’.
- Explore the decision making processes of Ethical Hackers.
- Identify structures of organisation within the Ethical Hacking community and examine the operation of these structures.
- Examine the career path, life course and motivations of the ‘Ethical Hacker’.
- Examine understandings of morality, ethics and legality with relation to Hacking and Ethical Hacking activity.

1.5 Theoretical Approach

The analysis of the decisions of the respondents to engage or not to engage in Hacking, to persist, or to desist is examined in this research making use of a ‘rational bounded model’ (Simon, 1957; Clarke and Cornish, 1985; Cornish and Clarke, 1986; Gigerenzer and Selton, 2001; Selton, 2001; Cornish and Clarke, 2008). This model utilises the ideas within Game Theory and within Rational Choice Theory regarding a reasoning individual, who makes decisions by weighing up the possible positive and negative outcomes, and the associated costs, but is removed from the mathematical modelling of Game Theory, and is removed from the political context and applications of Criminological Rational Choice Theory. Rationality is understood to be ‘bounded’ rather than comprehensive in that the choices available are seem to operate under constraint.

A Critical Realist approach has been utilised in designing the methodology for this study because realists “…have tended to assume that meaning, and mental phenomena in general, are real, rather than being simply theoretical abstractions” (Maxwell, 2012:1). Realism is compatible with a bounded rational model in that we are seeking to understand the generative mechanisms which underlie the decision making of the participants to this research.

This choice was made through an ontological realism which advocates that there is a real world independent of the researcher to be studied, but also through an epistemological interpretivism, which advocates that even though there is a real world to be studied, this is mediated through the interpretations of observers, including both the participants and the researcher. The methodological framework and the rationale behind it are fully explored within Chapter Four.

1.6 Additions to Knowledge

This research adds to pre-existing knowledge about Hackers by advancing a theoretical stance on a group which has not been examined in terms of its values, its social structures and their impact upon behaviour, or its development. The ‘Ethical Hacker’, it will be suggested, can be understood by considering attitudes and motivations, and by how and why skills and knowledge are developed. In particular a model for understanding Ethical Hacking will be produced which uses a rational bounded model (Simon, 1957; Clarke and Cornish, 1985; Cornish and Clarke, 1986; Gigerenzer and Selton, 2001; Selton, 2001; Cornish and Clarke, 2008) as a framework for understanding decision making in order to understand the events, careers and choices which characterise the Ethical Hacker.

The respondents revealed through their interviews that their decisions were made through a reasoning process whereby they attempted to maximise positive outcomes; decisions were framed ethically, morally or legally, or by some combination of all three. These issues, therefore, became the focus of the study with the attempt to utilise a rational bounded model as a framework for understanding these decisions and how and why they were made.

1.8 Chapter Outline

Chapter One has introduced to an area currently lacking academic engagement. The aims, objectives and research question have been outlined, along with a rationale for their development. The following Chapters will outline the relevant extant literature, the gaps in this literature and how these gaps may be addressed, who the respondents are, and the frameworks that influence their decision making.

Chapter Two will provide the historical context for the research. This Chapter will outline the history of computing, the internet and Hacking in order to show how and why ‘Ethical Hacking has developed in the way that it has. The literature which is available regarding Hacking, Hackers, Hacker social organisation and Hacker Culture will be examined. The majority of the research that is available concerns Hacking rather than Ethical Hacking, and is problematic in that it provides typologies of Hacking rather than theories which can predict or explain Hacking behaviour, however, it does begin to broadly frame some of the debates around Hacking which may be relevant to Ethical Hacking, so is useful in contextualising the area of study. Previous academic and scholarly literature will be examined, discussed and critically evaluated. The chapter will examine how the development of Hacking as an activity has created the need for the academic construction of the 'Ethical Hacker'. Underground, industry and academic understandings of Ethical Hacking will be utilised to introduce the research and to define the group of respondents to be studied.

Chapter Three will outline the development of regulation for cyberspace. It will outline the development of a legal framework for criminalizing Hacking in the UK including the formulation of statute, important cases, and amendments. The success of these amendments will be evaluated along with its implications of legislation for the industry as well as for the criminalization of activities and individuals. Alternative behaviour controls will also be outlined, including the use of computer code as a normative control, and the impact of personal approaches to morality and ethics. Virtue, deontological and teleological approaches to ethics are considered.

By discussing these normative and meta-ethical controls in relation to Cybercrime, a framework is created by which we can consider the perceptions of 'Ethical Hackers' in relation to what they perceive to be acceptable behaviour.

Chapter Four will outline the methodological choices made in this study of Ethical Hacking and the rationale behind these choices including, ontology, epistemology, sampling, methods of data collection, and data analysis. The chapter will begin to examine the theoretical implications of the choices made. It will focus upon the personal on social characteristics of the respondents and the highly sensitive nature of the topic of discussion. This chapter will consider issues raised by the choice of methodology and the implications for the research findings. The chapter will go on to consider difficulties arising within the research, how these have been dealt with and the implications for the research; this will include a critical discussion of the impact of the researchers' personal values and characteristics. The focus of the remainder of the chapter will include an extensive discussion of issues relating to validity, reliability and ethical issues. The benefits and limitations of the chosen methodology will be critically evaluated. Chapter Four outlines how Ethical Hacking has been researched in order to begin to close some of the gaps in knowledge that were identified in Chapters Two and Three.

Chapter Five will propose and explain a theoretical framework for understanding the 'Ethical Hacker' in relation to the current knowledge of the 'Underground Hacker', the defining characteristic being that the 'Ethical Hacker' is authorised or employed. It will be questioned whether all 'Ethical Hacking' may be defined as 'Hacking'. It will be questioned whether all 'Ethical Hackers' are actually perceived as being 'Hackers' within the field.

This chapter will show how Ethical Hackers themselves in relation to Underground Hacking, their world view, and their access routes into the field. Questions will be raised about why academia has constructed 'Ethical Hacking' differently to the common understandings within the computer underground. The bifurcated response of the security industry to the term 'Ethical Hacking' will be examined and its implications considered. In this chapter the responses of respondents to this issue will be explored.

Chapter Six will examine normative ethics including professional standards and the legal context and how these impacts upon the behaviour of Ethical Hackers. The distinct varieties of Hacker will be discussed in relation to their development and to their socialisation. The chapter will consider how respondents feel that the legal framework has impacted upon their own personal choices about behaviours and will go on to discuss the perceptions of respondents regarding whether legality is important to them, or to the 'Underground Hacker'. The legal framework will be presented as a social construction related to the media criminalization of Hacking and the impact of this upon public perceptions of Hacking as an activity. It will be questioned whether the legal distinction is the only distinction between the 'Underground Hacker' and the 'Ethical Hacker'; other potential differences will be discussed.

The chapter will go on to outline meta-ethical theoretical and philosophical approaches to moral and ethical behaviour and will examine the narratives of respondents in the light of these. Ethical stances which focus upon the intentions and actions of and individual, and also the consequences of action then be explored. The decision making of Ethical Hackers in relation to individual Hacking events, and also ongoing careers, persistence in criminality and desistance from criminality will be examined. The development of personal moral and ethical stances will be examined, along with a discussion of how these have affected choices in the career paths, personal development and behaviour of respondents.

Chapter Seven will outline the findings in relation to the historical, theoretical, legal, and political context in order to conclude the research. The decision making processes of Ethical Hackers in relation to these will be detailed. The research and literature will be briefly summarised and the implications for further research will be explored. The impact of the study will be considered for policy makers, for both Ethical Hackers and Underground Hackers, for educational professionals, and for employers.

Chapter 2: The Development of Hacking

2.1 Introduction

"…the world opened up by the computer was a limitless one"

(Levy, 1984: 230)

This chapter provides the historical context for the study. The chapter begins by outlining the origins and development of computing, the internet and hacking. The definitional issues around the nature of the terms 'Hack' and 'Hacking' will then be addressed, followed by an examination of recent attempts to typologise the Hacker in terms of the associated attributes and characteristics.

Chapter Three will then build upon this history by examining attempts at theorising and typologising Hackers. This historical review begins with an exploration of the origins and development of Hacking as an activity, and as a social phenomenon. This creates a contextual background against which the development of Ethical Hacking is introduced

2.2 Origins and Development of Computing, the Internet, and Hacking

The development of computing, networking and Hacking are very much interdependent phenomenon (Hafner and Markoff, 1995) as will be shown later in this chapter. Computers in the 1950s had developed into the huge mainframe machines, which were in use at Massachusetts Institute of Technology (MIT) when the term 'Hack' first came into general use. Levy (1984) explains that in 1959, MIT housed an early IBM 704 in the Electronic Accounting Machinery Room. Early Hackers, MIT electronic engineering students (McQuade, 2006) from the Tech Model Railroad Club (Schell and Martin, 2004), broke into the room after hours in order to spend time programming the 9-foot-tall (2.7 m) 30 tonne machine. The students involved saw Hacking as a pleasurable activity rather than one with a constructive goal (Levy, 1984). Before the term Hacking was adopted to mean pleasurable and harmless computer intrusion, as it was understood in the 1950s, it was used to describe the pranks and jokes that the college students would carry out as well as some of their problem solving activities (McQuade, 2006). It was not until much later that the term came to be demonised by the press, and in the popular imagination.

> Computer programmers from the 1950's and 1960's…saw their work as breaking new ground by challenging old paradigms of computer science, think of hacking as an intellectual exercise that has little or nothing to do with the exploits of their 1980s and 1990s counterparts.
>
> (Thomas, 2002: ix)

A number of research projects during the 1960s and 1970s began to focus on connectivity between physically separate systems. These included the laboratories of Vinton Cerf at Stanford University, Donald Davies (NPL), Paul Baran at RAND and Leonard Kleinrock at MIT and at UCLA. Digital networking developed using a system called 'packet switching' whereby packets of data are exchanged and reassembled. The research initiated the inception of a range of packet-switched networking solutions in the late 1960s and 1970s, including ARPANET, Telenet, and the X.25 protocols (Hafner and Lyon, 1998).

The Advanced Research Projects Agency (ARPA), with funding from the US Department of Defence, installed ARPANET at UCLA in 1969 (Weber, 2003; Hafner and Lyon, 1998). It was marketed, although not initially intended, as a communication system that would be able to survive a nuclear attack (Hafner and Lyon, 1998), with a protocol that originally allowed a maximum of 1,000 users. On October 29, 1969, computers at Stanford and UCLA linked online for the first time. The first ever message to be sent was intended to say the word 'login'; however the system has been widely reported to have crashed on the letter 'g' (ibid, 1995). As the network was initially only used for ARPA research purposes, it was not designed with security in mind, it was designed to be open, to be robust and to be flexible. The network initially linked only a few government and university PC's and was used for simple tasks including e-mail, remote connection and e-newsgroups. By 1971, the ARPANET network linked approximately fifteen nodes, with the first international connections made in 1973 (Weber, 2003). Where ARPANET was a single network, the internet was destined to be a network of networks. In 1989, ARPANET became the 'internet' with the addition of a number of other networks, at this time over 100,000 host PC's were linked to the network (Weber, 2003) In the early 1970s technologies that allowed people to use de-centred, distributed networks of computers to communicate with each other were developed alongside the development of hardware (Levy, 1984). Late in the 1970s, a means by which the different networks of computers could be connected to each other was developed, the Internet, and a worldwide network of computers became a reality (Hafner and Lyon, 1998; Quarterman, 1990). TCP/IP, the protocol which allowed this was first used in 1983 on ARPANET at which time MILNET replaces ARPANET in the hosting of military networks (Weber, 2003).

Public and hobby networking solutions began to become popular including FidoNet, and unix-to-unix copy (UUCP). They were still separate networks, served by only a small number of access gateways between networks. This led to the application of packet switching to develop a protocol for internetworking, where multiple different networks could be joined together into a super-framework of networks.

Adoption and interconnection occurred quickly across the advanced telecommunication networks of the western world, and then began to penetrate into the rest of the world as it became the de-facto international standard for the global network. However, the disparity of growth between advanced nations and the third-world countries led to a digital divide that is still a concern today (Sassi, 2005).

The internet has also developed along corporate lines. This commercial network includes uses such as advertising, promotion, and sales. In 1972 AT&T declined control of the network as they felt that it lacked in profitability (Curran, 2010); even later when funding did become available, control of the network was declined again by AT&T (Hafner and Lyon, 1998). It was not until the late 1980s and early 1990s that the commercial value of the network was eventually widely realised. 1995 was a significant year for the commercialisation of the internet; secure methods for making online payments led to a boom in online trading with many of the websites which have become international trading institutions emerging. Echo Bay (e-bay) and amazon.com were both started up in 1995. The increase in members of the public buying goods online in turn raised awareness of and paranoia regarding internet security. Sites which for many have come to be first sources of information soon followed; Google was initiated in 1998, followed by Wikipedia in 2001 (Jewkes and Yar, 2010). Google and Wikipedia's popularity have added to the exponential increase in the use of the internet, taking use to a daily, or in some cases even an hourly experience. As more people became comfortable using the internet more outlets to buy products came online. This increase in cyber trade meant that what Berners-Lee

(1995) had hoped would be a free source of information became commercial in a way that had never been experienced before.

> Tim Berners-Lee made the source code for the first World Wide Web browser freely available as open-source software. The subsequent development of the public Internet was, however, marked by the early dominance of the commercial Netscape Navigator browser which, in turn, gave way to the Internet Explorer browser that Microsoft gave away 'free' with every copy of their windows 95 operating system.
>
> (Athique, 2013: 143)

This characteristic commercialisation was net-wide, and led to opportunities for theft via illegal Hacking, identity theft and fraud, which in turn created the need for internet security specialists.

The MUD (short for Multi-User Dungeon) was created in 1979; these were entirely text-based virtual worlds which combined role-playing games, interaction, fiction, and online communication. 1979 also saw the birth of UseNet. Created by two graduate students, UseNet allowed people to post public messages to newsgroups. There developed a range of MUDs, MOOs (an object-oriented version of the MUD (Dibbell, 1998), Bulletin Boards (BBS) Usenet groups, chat-rooms, social networking sites, and virtual communities (Laurel, 1991; Wellman, 1999; Rheingold, 2000; Hampton and Wellman, 2003; Hargittai, 2003). The WELL (whole earth lectronic link) is one of the oldest online communities. Stewart Brand and Larry Brilliant launched it in 1985 (Curran, 2010). Facebook (originally 'The Facebook') was started up in 2006 (Jewkes and Yar, 2010). The increase of e-commerce and social media has increased both internet use and concerns about the security of data.

The World Wide Web (www) was designed to allow all of the machines from the various different networks to connect to one another, as Tim Berners-Lee, the creator of the www protocol describes, the design was open, rather than being security focused. He states that “The web’s major goal was to be a shared information space through which people and machines could communicate. This space was originally intended to be inclusive, rather than exclusive” (Berners-Lee, 1996: 69).   Because of the unwelcome commercialisation of the internet, a number of 1990’s Internet Hackers began the creation of what was termed ‘Internet 2’; this is not commercialised and is a network that is mainly utilised by researchers and HE organisations (Van Houweling and Hanss, 2005).

Tim Berners-Lee who wrote the protocols for the Worldwide Web (www) did not see this as a profit making enterprise; rather, in line with the ethics of the FOSS movement, he was driven by the desire to disseminate something that would be useful and would be empowering to the whole of society (Curran, 2010; Berners-Lee and Fischetti, 1999; Berners-Lee, 1996, Athique, 2013). Users of the internet had another visualization of a potential future that was offered by the new landscape; it was perceived to hold the potential to allow the construction of new ‘virtual’ interactions, and online communities. This would alter and expand our social interactions, giving global capacity to our experience of society.

This optimistic and utopian vision of the computer underground with regard to the potential positive capacity of the use of networked technology soon gave way to a range of fears and anxieties within society (Mordini, 2007), some rational, some irrational. The exponential growth of a global network of machines and the increasing use of these machines in the creation of virtual online worlds and communication has had a major impact on our understanding of the social; we have had to redefine our understanding of pre-existing social worlds. The anonymity offered by these cyberspaces and their communities allowed the citizens of the internet new opportunities for deviance (Wall, 2010; Tavani, 2004) – new forms of deviance have zemerged alongside new methods of committing more traditional forms of deviant or criminal behaviour (Wall, 2007; Walden, 2011). This has led to a number of disparate attempts to regulate cyberspace (Wall, 2007), this will be examined in detail in the following chapter.

The Hacking community has derided the unfortunate claiming of cyberspace as a new market; commerce was quick to move in as there were opportunities for making huge profits due to the global reach of the network. Part of the ethical stance of Hackers is to share resources and information for the benefit of all (Levy, 1984; Himanen, 1991; Wark, 2004), so commercialisation was not acceptable to the Hacking community. The internet was created out of public funding and developed largely by the Free Open Source Software (FOSS) movement, and therefore it is arguable that it should have remained free and un-commercialised. The FOSS movement sees software as something to be shared so that it can be efficiently improved by any individual who has the motivation and the skills to do so. "The free software movement sees programming as a linguistic resource, like the English language, that belongs in the public domain" (Athique, 2013: 146). FOSS will be further examined in the following chapter.

2.3 Understanding 'Hacks' and 'Hackers'

The nature and definition of Hacking is highly contested. Ross (1991) offers a range of definitions which are indicative of this:

> a) Hacking performs a benign industrial service of uncovering security deficiencies and design flaws.
> b) Hacking, as an experimental, free-form research activity, has been responsible for many of the most progressive developments in software development.
> c) Hacking, when not purely recreational, is [a sophisticated educational practice that reflects the ways in which the development of high technology has outpaced orthodox forms of institutional education.
> d) Hacking is an important form of watchdog [countervailing] the use of surveillance technology and data-gathering by the state, and to the increasingly monolithic communications power of giant corporations.
> e) Hacking, as guerrilla know-how, is essential to the task of maintaining fronts of cultural resistance and stocks of oppositional knowledge as a hedge against a technofascist future.
>
> (Ross, 1991: 81-2)

Both terms seem to be relative to their context, and to provoke a variety of connotations in different social environments, depending upon how the meanings have been socially constructed over time, and by whom. According to Thomas (2002) the term ‘Hacker’ is difficult to define due to the fact that it:

> …has been stretched and applied to so many different groups of people that it has become impossible to say precisely what a Hacker is. Even Hackers themselves have trouble coming up with a definition that is satisfactory, usually falling back on broad generalizations about knowledge, curiosity, and the desire to grasp how things work.
>
> (Thomas, 2002: 5)

As outlined in the previous chapter technology has developed rapidly since ‘Hackers’ first emerged. The growth of Hacking as an activity, along with other forms of cyber-crime and cyber-deviance, has mirrored the exponential growth of technology and the development of the internet. Contemporary approaches have focused on personality profiles and on the changing nature of Hacking as an activity. In order to understand the Ethical hacker it may also be useful to consider the nature of Hacking as a philosophy or as a set of ethics rather than simply as an activity.

Once the telephone capacity was being utilised for computer-mediated communications, the next logical step was to manipulate this new form of data being transmitted on the copper wires. New technology has created new opportunities for social interaction, and for commerce, and therefore new opportunities for the commission of crime.

The creation and expansion of the internet has created the opportunity for hacking to grow and to diversify, as more people have the access and the knowledge required.

Given the difficulties surrounding defining the nature of a 'Hack', it becomes apparent that the 'Hacker' is difficult to define in relation to a clearly defined set of activities or behaviours. A 'Hack' is now generally understood by the ordinary public to mean breaking into a computer particularly in order to steal or damage - the 'Hacker' is therefore defined as being the perpetrator of a Hack. The meaning of the term 'Hacker' has altered significantly since its conception, and it is used differently according to the meaning constructed within the particular context; as previously outlined in detail within Chapter Two the available literature regarding Hackers does not always describe the same social group (Denning, 1990; Hollinger, 1991).

The 'good' Hack has been defined by the presence of three main elements, these being simplicity, mastery and illicitness (Turkle, 1984); As Bachmann says (with particular reference to 'black hat' hackers) "…they engage in illicit activities, a circumstance that introduces greater risks, raises the stakes, and increases the excitement and thrill…" (Bachmann, 2010: 644). The Hack should be done by the most efficient means possible, should be done well, and should be something that is somehow deviant according to this conception. A Hack is more highly valued on its first usage than subsequent ones; it loses status each time it is copied, and the more closely it is copied (ibid, 1984). The Hack is therefore seen as an aim in itself, rather than simply being a process which leads to the achievement of some other outcome.

It is not uncommon for Hackers to desire the knowledge of how to steal, or to access forbidden data, but then once the knowledge is gained, not to use it. Understanding the Hack in itself helps to explain why Hackers rarely damage or change the data or systems that they access. For many, it is the ability to manipulate technology, and the belief that technology can be bent to new and unanticipated uses that defines the Hack, and therefore the Hacker, rather than its products or outcomes (Levy, 1984; Turkle, 1984; Jordan and Taylor, 1998; McQuade, 2006).

Conceptualising the 'Hacker' is complex (Hollinger, 1991). Logically, a Hacker must be defined as being an individual who Hacks, someone who engages in the act of Hacking. The on-line Hackers 'jargon file' (http://catb.org/~esr/jargon/html/, no date) defines the activity of Hacking as, "…engaging the act of programming enthusiastically (even obsessively)". The meaning of the term has however changed and has diversified over time (Taylor, 2000; Kleespie, 2000; McQuade, 2006) and is used in many contexts in order to describe a complex mix of both legal and prohibited activities.

The activity of Phreaking preceded Hacking (Sterling, 1992, Hollinger, 1991); this consists of attempting to illicit free telephone calls and to impress other phreaks by performing 'clever tricks'. Steve Wozniak and Steven Jobs (Apple Computer, Inc) once dabbled in 'blue-boxing', which is a form of phreaking, the blue box would trick the exchange by sending a signal down the line which would allow free long distance calls (Sterling, 1992; Edgar-Neville and Stephens, 2008) Hackers will usually know how to phreak, though they will often perceive this as a lower level activity; they perceive it to be a less technical activity than hacking (Sterling, 1992) and therefore carrying lower social desirability in the Hacking community (Meyer, 1989). Phone phreaks often do not fully engage with Hacking as an activity, but may partially engage in order to gain knowledge and skills. The lines between phreaking and Hacking have also come to be more blurred now that much of the telephone system is digitalized and computers also have voice transfer capabilities. The technologies are interconnected, and therefore become interchangeable. This is seen as being a major development in the creation of the phenomenon of hacking as we know it as Hafner and Markoff (1995) describe:

> When the personal computer was invented and mated with the modem, phreaking took on a whole new dimension and the modern age of the Hacker was born.
>
> (Hafner and Markoff, 1995 as cited in Fafinski, 2009: 20)

Due to developments in technology, and in society, hacking is rising in incidence whilst it is simultaneously diversifying in mode and motivation. It is now a topic of major significance within the social sciences; social researchers have attempted to contribute to our understanding of the Hacker, and of the social environment in which he operates, both of which will be examined within this chapter. Hacking is now variously perceived to be the act of computer intrusion, the act of bending technology to new and unanticipated uses, excessive computer programming or has also been viewed as a set of values and motivations that underpin an activity rather than the activity itself depending upon which literature is consulted. Jordan and Taylor tell us that "…It is the belief that technology can be bent to new unanticipated purposes that underpins hacker's collective imagination" (1998: 764). The computer is malleable in its logic, which makes it useful for a range of purposes (Moor, 1995). Hackers can be defined by their intent to exploit this malleability in order to create new possibilities. The diversification of 'the hack' has in turn led to complications with formulating a true typology; those that have been created tend to be partial, or to compete. The following section outlines some of the recent attempts.

2.4 Hacker Typologies

As described in the previous chapter, the term ‘Hacker’ developed in the 1950s at MIT (Levy, 1984; 2002), it was originally used to mean a person who was able to use technology for a purpose for which it was not originally intended. “Since that time Hackers have been variously defined as individuals possessing extraordinary curiosity about, enthusiasm for, and expertise in computer programming” (McQuade: 2006: 232). The media have been blamed for the later demonization of the Hacker (Kirkpatrick, 2004; Kleespie, 2000), and for the negative, pathological and criminal connotations that the word now carries for many. Kleespie (2000 discusses the impact that the media have had on the meaning of the word, stating that:

> Media coverage has given the term ‘Hacker’ a negative connotation. However, the original usage was complimentary, indicating someone with a high level of technical sophistication, or someone who enjoyed the intellectual challenge of overcoming or circumventing limitations.
>
> (Kleespie, 2000: 1)

The impact of this is that:

> …the general public tends to stereotype hackers as clever, yet sinister computer criminals who essentially live in cyberspace where they go on thrill-inducing missions to exploit vulnerabilities in other networks and systems…this is greatly oversimplified…
>
> (Bachmann, 2010; 644)

Life in cyber-space seems to be alien and abstract to those who are outside of it; society is fearful of these individuals who operate mainly in cyberspace; they often seem to be described as being outside of mainstream society and to be incapable of functioning within it (Dibbell, 1998). The fear of the power of computers over social life, and the ability of the Hacker to control and manipulate the computer systems upon which we all rely compounds and exaggerates this terror. The anonymity that makes the Hacking community difficult to study, in turn creates a social space for such pathologizing to occur. The available literature often typifies the Hacker as being someone who is obsessed with computers, is socially isolated, and is lacking in social skills, (Hollinger, 1991; Post, 1996; Boni and Kovacich, 1999: Lilley, 2002a).

The literature portrays the Hacker as being in many ways pathological; many people have come to believe that Hackers lack the ability to communicate effectively in offline space, and that they therefore tend to display sociopathic tendencies, with many of them preferring the company of machines to other people. Hackers have been pathologised in many ways, including them having been described as being obsessive compulsive (Dreyfus, 1997). Hacking as an activity has also been linked with the autism spectrum disorder Aspergers Syndrome, which increases the tendency towards obsessive behaviour. Hacking has also been associated with depression and a sense of inferiority, the suggestion being that the activity and the social network associated with it increases self-esteem (Fotinger and Ziegler, 2004).

Hackers have often been perceived to be introverted, friendless individuals (Hollinger, 1991 Post, 1996; Boni and Kovacich, 1999: Lilley, 2002a) who have sought solace in the company of machines, or who cannot socially interact without the anonymity offered by cyberspace. This is a major error on two counts. Firstly, the Hacker, contrary to popular perceptions and common understandings, has the tendency to prefer Hacking in groups. They relish the status that they perceive within a clever Hack, (Turkle, 1984; Sterling, 1992) and need information sharing networks both to advertise to others what they have done in order to gain this status, and they also utilise these networks in order to develop their own capacity through information sharing (Arquilla and Ronsfeldt, 1996). This can include both corporeal and virtual relationships though most often it will include both (Sterling, 1992).

Levy (1984) outlines the set of ethics which he feels that Hackers share in common with one another, and which it is suggested define the hacking community. The general principles of the Hacker ethic include sharing, openness, decentralization of power and technology, and social advancement (Levy, 1984; 2002; Wark, 2004).

Levy (1984) attempts to conceptualise the Hacker and to trace the development of Hacking through three 'generations'. The early computer pioneers of the 1950s and 60s are referred to as 'True Hackers', while their 1970s counterparts, who idealized personal computing and the decentralization of technology, are alluded to as 'Hardware Hackers'. Finally, according to Levy's chronological characterizations, are the 1980s 'Game Hackers' who hacked electronic gaming applications. Parker concluded a study in 1996 on more than 80 UK and US Hackers and suggested that in his opinion, and based upon the interviews conducted, Hacking had come to be seen as being more malicious and less honourable an activity than the image that had been portrayed by Levy in 1984. This negative perception may be unsurprising given that the respondents to the study were known to be criminal hackers, and therefore unlikely to be representative of the less malign factions who work for free in developing software to be openly shared for example.

Sterling (1992) outlined the history of Hacker culture in the late 1980s, and of the successful law enforcement efforts to prosecute Hackers culminating in crackdowns in 1990. Sterling suggests that the struggle between Hackers and law enforcement is a struggle for power. The relationship between Hacking and power will be examined later in this chapter in order to help us to better understand the nature and organisation of the Underground Hacking community, and to provide a context for a discussion of the social organisation of the Ethical Hacker within Chapter Five.

Jordan (2009) believes that the three groups who make up the Hacking community determine the underlying nature of Hacking. These are Hackers who break into systems (often termed the 'Cracker'), Hackers who work on open source software development (FOSS), and Hackers who see Hacking philosophy and politics as the essence of 21st century creativity. The FOSS movement is considered to be the direct descendant of the ethics outlined by Levy (1984). The access to open source software which is silently agreed upon as a cultural value for FOSS Hackers is seen as essential to the development of software solutions.

Taylor (2000) concurs with the categorizations created by Levy (1984) and adds three new categories; he describes malicious or criminal Hackers as 'Crackers', those who work in the computer or telecommunications industry as 'Microserfs', and also describes a group that he calls 'Hacktivists' who, it is suggested, Hack for political gain (Taylor, 2000). The terms 'Cracker' and 'Hacktivist' are now both in common use within the community, the field in general, and in the media. In Taylor's own words:

> Hacker/Crackers: from the mid 1980's to the present day, both these terms are used to describe a person who illicitly breaks into other people's computer system…
> Microserfs: in Douglas Coupland's novel of the same name, microserfs is the word used to describe those programmers who, whilst exhibiting various

> aspects of the hacker subculture, nevertheless become co-opted into the structure of Microsoft or any similar corporate entity.
> Hacktivists: the mid 1990's marked the merging of hacking activity with an overt political stance…
> (Taylor, 2000: 61)

Lilley (2002a) suggests that the ethic apparent in Levy's (1984) seminal work on Hackers is still useful to analysts in understanding the motivations and the behaviours of Hackers; the categories outlined by Lilley (2002a) support the typologies created by Levy (1984) and Taylor (2000).

According to Boni and Kovacich (1999:76) by the late 1990's Hackers were predominantly Caucasian, were generally male, were young (typically aged 14 – mid 20's), they were very intelligent, were likely to be devoted computer enthusiasts, and were introverted and insecure (which is later supported by Lilley, 2002a, as described above); they tended to be from middle to upper middle income family in line with the costs of the technology at the time. This class distribution may not now be as predominant since the proliferation of low cost technology, but is still thought to be an issue. It is certainly an issue on a global scale. It is of note that the more negative of the descriptors given within the typologies tend to based on subjective judgments and can therefore be criticised for lacking in scientific rigour.

Other writers have concurred that Hacking, as with other computer mediated activities, has come to be perceived as a predominantly male behaviour (Schell and Martin, 2004) which would appear to be in direct conflict with the 'Hacker Ethic' as outlined by Levy in 1984, showing that this was not a universally or uniformly accepted set of standards.

Other writers have offered typologies of Hackers that are based upon their motivations, rather than the personality profiles or demographic characteristics as many previous attempts at profiling had. The categories outline by Cherilla (2002) for example include the 'Communal Hacker' who is driven by the need to gain acceptance from the community, the 'Technological Hacker' who is driven by the desire to find new uses and fully exploit the potential of technology, the 'Political Hacker' who has some message that he wants to pass on to wider society and the 'Economical Hacker' who is driven by a desire for financial gain. This is useful, as it helps us to understand that in attempting to define the Hacker, we are not always describing the same individuals or behaviours. It is also useful in understanding some of the motivating factors in Hacking behaviour.

Hackers are commonly described as being either 'white' or 'black' hat Hackers. (Schell and Martin, 2004, Graves, 2007) According to Schell and Martin (2004) this formulation denotes whether they have good or bad intentions, and is based on early western films, where the 'goodies' wear white hats, and the 'baddies' wear black.

> ***White Hats*** are the good guys, the Ethical Hackers who use their Hacking skills for protective purposes. White-hat Hackers are usually security professionals with knowledge of Hacking and the Hacker toolset and who use this knowledge to locate weaknesses and implement countermeasures.
> ***Black Hats*** are considered the bad guys: the malicious Hackers or *crackers* use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote machines, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and basically cause problems for their targets.
> ***Gray Hats*** are Hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Both arepowerful forces on the Internet, and both will remain permanently. And some individuals qualify for both categories. The existence of such individuals further clouds the division between these two groups of people.
> (Graves, 2007: 6-7).

As we will see in chapter 5, this may be more appropriately viewed as a spectrum of shades of grey in relation to the Ethical Hacker.

These descriptions are among numerous attempts to profile or to categorise the Hacker; and therefore must be understood within the confines of the time, the cultures and subcultures and the individual biases that have influenced and shaped their development. They range from very positive descriptions such as those from Levy (1984) and Taylor (2000) to very negative views, such as those from Parker (1998), and Boni and Kovacich (1999). A particularly extreme perspective was suggested by Rosenblatt (1996) who attempts to establish a relationship between the Hacking community and paedophilia/ snuff films.

A more recent research project, commenced in 2006, and still currently ongoing, is the 'Hacker Profiling Project '(HPP). The project was commenced by Raoul Chiesa, a reformed black hat Hacker, who was later joined by criminologist Stefania Ducci. The aims of the project were to aid with crime prevention by producing profiles of Hackers based on a self-report survey carried out both on and offline and then collating these profiles with information gained from a honeynet. The ultimate goal was to sell a profiling service, which provides a profile of the Hacker, which is based on the evidence gained about his methods during an attack. The Hacker Profiling Project employed a multi agency approach, which involved the participation of the Hacker underground, but also private companies and academics. The research initially was aimed, according to the lead researchers, to balance out the approach to the study of Hackers, which has tended to be very one-sided in its approach in the past. Hackers are encouraged to participate in order to reduce the social stereotypes, largely created by the media and popular fiction, which in recent years have come to cast the Hacker as being criminal or deviant.

Chiesa acknowledges that there is an issue of validity around the sampling of the self-selected respondents to the online survey (www.isecom.org/hpp/, no date). Firstly, they have to know about the project. Most Hackers probably will have an awareness of the project; its aims, its progress, and its validity have been widely discussed on Hacker forums and in Hacker literature available online. Any basic search that includes the term 'Hack' or 'Hacker' will bring up the project quickly. The next issue is that respondents have to self select to complete the survey. The tri-part survey is relatively short, but there is no incentive other than the reduction of negative stereotypes to incite the Hacker to take part. In fact there may be a direct disincentive for criminal Hackers as one of the stated aims is to provide profiles to security experts to help them in reducing cybercrime by understanding who Hackers are and why they engage in Hacking. It is well known that a character trait of many Hackers is the need to brag or show off in order to gain status, which may lead some to be dishonest or to exaggerate in their survey responded. Hackers who are committing serious crimes, are engaged in state sponsored espionage, or those who are very experienced and knowledgeable will be the least likely to take part. This may mean that the self selected sample lacks reliability and therefore generalisability to the wider population. In order to resolve this issue, Chiesa chose to create the honey-net; a set of networks designed to entice Hackers to break in, and then record their movements while inside the systems in order to build up an empirical understanding of the methods employed.

While the project may produce some very valuable information on criminal Hackers (or crackers, as they would be termed by the Hacking community) it does not focus on individuals who employ Hacking skills in a legal or authorised setting. It does discuss "Ethical Hackers" but employs the original underground sense of the term, before it was accepted within academia in its current sense; the Ethical Hacker is understood here as being a Hacker who breaks the law, but who does so for an ethical purpose.

The Hacker typology that has been created by ‘The Hacker's Profiling Project’ suggests nine ‘pure’ or ‘ideal’ types of attackers, it is acknowledged there may be some overlaps between the categories and that some Hackers may not fit neatly into the typology:

> Wannabe (Lamer) Attackers of this category use hacker techniques without learning how they actually function. They use “hacker toolkits,” which can be downloaded for free from Internet.
>
> Script kiddie Script kiddies base their perpetration on UNIX/Linux shell scripts written by others. They lack technical skills and sophistication.
>
> Cracker Crackers have good technical skills, which allow them to pursue their purposes.
>
> Ethical Hacker An “ethical hacker” is somebody with excellent hacking skills, who decides to help, digging with software and discovering bugs and mistakes in IT infrastructures, protocols or applications.
>
> QPS (Quiet, Paranoid, Skilled Hacker) The QPS are creative hackers, using as little as possible software made by others, since they prefer creating them by themselves.
>
> Cyber-warrior/Mercenary This categories of attackers appeared in the last few years because of Internet’s globalization. Cyber-warriors feel like heroes from their own environment. They work on commission, getting money to attack specific targets.
>
> Industrial Spy Hacker Traditional industrial espionage is now using Industrial Spy Hackers, which modernized this practice taking advantage of the new opportunities brought in by Information technology.
>
> Government Agent Hacker This category of attacker run highly-sophisticated attacks, specifically focused towards nations’ know-how in different business markets.
>
> Military Hacker This profile is associated with the term “state-sponsored attack,” which effectively represents the logic and the approach behind those attacks run by Military Hackers
>
> (www.isecom.org/hpp/, no date)

2.5 Hacking: Affordance and Determinism

More recent approaches to Hacking have begun to move away from the negative and pathologised view of Hacking as an activity and have begun to focus upon the relationship between Hacking, social evolution, and technological development (Lilley, 2002; Wark, 2004; Himanen, 2001). This takes our understanding of the concept of Hacking back towards its original roots at MIT (Levy, 1984; Sterling 1992, Turkle, 1984). Cyberpower is perceived to be a collective as well as an individual phenomenon, in that social worlds are instrumental in defining the ways in which people act so that “Cyberpower of the social derives from the belief that individuals have their possible actions defined by the collective bodies of which they are part” (Jordan, 2009: 5).

Hacking is also seen as a revolutionary force (Wark, 2004; Hollinger, 1991), rather than as a pure business or production model. It is suggested that Hacking creates the opportunity for innovations in common with the view suggested by Himanen (2001). In seeing Hacking as something which creates something different and new these perspectives do not provide us with knowledge that is specific and so the nature of Hacking must be considered in more depth. They are also ungrounded in empirical evidence, and therefore require support from other commentators.

An essentialist technological determinism is possible; the state of a society’s technology is perceived by some to be crucial in defining its social nature; technical change is the most common determining factor of social change (Winner, 1997). This view however oversimplifies the nature of society, and whilst technology is an important factor of determinism other factors such as the economy or social discourses may be equally important. As the Hacker is responsible for the technological advancement, the determinism is both technology-driven and hacker-driven. Hutchby (2001) discusses the concept of affordance in order to show the limits of this determinism. Determinism does not produce a particular or linear result, but rather a range of potential outcomes. The technology offers a range of possible opportunities or future directions to be taken, but these opportunities are limited by the range of capabilities that are inherent within the technology.

Society may determine technology as much as technology determines society in that technological advances are shaped by needs and desires (Hutchby, 2001). The fulfillment of needs and desires by the creation of new technologies creates further social opportunities. An example of this is the creation of the internet, which arose from the need and desire for networked technology for research and defense purposes (Hafner and Lyon, 1998). Once the technology was developed, new social opportunities were created. These new social relationships have created new social groups, which have then contributed to further developing the technology. So the social and the technological therefore determine one another in an ongoing cyclical pattern and the role of the Hacker in creating the new and the different has been at the core of this development and determinism. Technologies are open to recycling, reinterpretation, and amendment, but only within a particular range of possibilities (Hutchby, 2001). The overall meaning of Hacking therefore appears to be the renegotiation of society and technology within a range of determinisms and affordances. The power of the Hacker is the power to produce change by creating new possibilities for further change. The Hacker then creates another new set of possibilities from within the previous affordances in an ongoing cycle. In the case of Hacking it would appear that determinism is both socially and technologically driven.

The Hacker creates new technology, and this technology creates a whole new range of possibilities to be exploited by other Hackers.

Himanen (2001) examines the nature of creativity, which is seen as being the quintessence of Hacking. Creativity is described as being the most important aspect of Hacking, but also listed are six other characteristics: passion, freedom, social worth, openness, activity, and caring (cited in Jordan, 2009). Hacking is perceived to be any inventive and inspired use of one's own abilities that creates something novel, and therefore provides the social world with creative new innovations. These characteristics constitute a new way of working, which is non commercial and is therefore focused on solutions rather than upon profit; this can produce innovations quickly, effectively and collectively.

The FOSS movement is a creative Hacking movement which advocates the development of free open source software, which can be accessed and modified by anyone. During the 1990s the media focused very heavily upon cracking as the main form of Hacking. The move back towards the FOSS movement is a move back towards the original sense in which the term was used. "Open source is not a new way of doing things— it is the original computer way of doing things" (Rosenberg 2000: 3).

The operating system Linux, developed by Linus Torvalds is a well-known example of open source software. It, along with other open source software, is commonly used by Hackers, and is perceived to be in many ways superior to commercially developed software. What does however become apparent from a closer examination of the community surrounding the creation of Linux is that FOSS is not as 'open' as it at first may appear to be. The volunteers who debug and modify the software are not final editors; this position is retained by Torvalds himself. As the operating system has grown over time, Torvalds has delegated some of this responsibility to a series of lieutenants who take responsibility for separate areas of functionality. This creates a hierarchical, rather than an open, networked or flat organizational structure. This provides support for Jordan's (1999) conception of the formation of a techno-elite who can have social and political power because of their technological skills and expertise. It does not however fit well with the Hacker Ethic outlined by Levy (1984): despite status being derived from skill, information is not freely shared.

Jordan (2009) suggests that FOSS alters our perception of ownership from being the right to exclusive use, to the right to distribute. What Cracking and FOSS have in common are innovation, computing, and social and technological determinism. It is vital to keep in mind the dynamics of Hacking as well as the skills that are commonly supposed to be its more evident markers, if we are to come to understand it.

Community, technological and social determinism, the created affordances, creativity and innovation define Hacking. It includes cracking and FOSS within it's current main strands, but also includes a diverse range of other personalities, motivations, and activities. The Hacker is a skilled individual with the power to produce social and/ or technological change. This may not always be change for the better, but does always produce difference or novelty so can be perceived as being a kind of socio-technical evolutionary force. The social organisation of the Hacker is as a virtual (Rheingold, 1993) and as a real community, which has revolutionary capacity (Wark, 2004; Hollinger, 1991) within a range of afforded possibilities (Jordan, 2009). This community will continue to grow and to diversify in the future as the capabilities of the technologies develop.

Hacker social organisation is further examined in the following section in order to contextualise the discussion of Ethical Hacker social organisation within chapter 5.

2.6 Hacker Social Organisation

Jordan and Taylor (1998) toy with the concepts of ‘social movement’ and ‘subculture’ in their discussion of the social organisation of computer Hackers but the dominant description that is utilised is of a ‘community’, “…a community whose aim is to hack…” (1998: 760). They define community as being “…the collective identity that members of a social group construct...the ‘collective imagination’ of a social group.” (1998: 762-3). Anderson (1991) describes an ‘imagined community’ who have an imagined collective identity even though the individual members may never actually meet. Hackers see themselves as a separate community; “…Hackers negotiate a boundary around their community by relating to other social groups…” (Jordan and Taylor, 1998: 770); these groups would include the media, the public, and computer security experts.

The social organisation of Hackers is generally described as either a ‘community’ or a ‘network’. According to Jordan and Taylor (1998: 758) “…computer intrusions come from a community that offers networks and support…”, a virtual community which is structured and organised around an interlinking set of networks because of the way in which it emerged and developed. It may be that the social organisation of Hackers is best understood as a number of separate and sometimes overlapping communities rather than as a single coherent community (Jordan and Taylor, 2004).

This is a useful conceptualisation which we will consider in relation to the social organisation of Ethical Hackers in relation to the wider hacking community within chapter 5.

It has been suggested by some that online communities cannot offer the genuine relationships which are to be found in offline environments (Parks, 1996; Beniger, 1987) some commentators have went further and have even argued that social isolation is actually more likely as a result of the development of online social relationships (Kiesler, Siegel, and McGuire, 1984) due to the less intimate level of social bonding which takes place.

Lockard (1997) disputes the existence of online communities, pointing out that virtual communities do not fit general understandings of the concept of community as they do not share a geographical space, and do not perform all of the functions of a community. Lockard (1997) takes a very pessimistic view as to the nature of online communications, seeing them as distant, depersonalised, and inferior to real relationships. Rheingold (1993) disagrees, he suggests that the community to be found online, although virtual is none-the-less “real”, and that the increase in the numbers of virtual communities is a result of the need that people have for the ‘social’. Jones (1995) shares the view with Rheingold (1993) and Oldenburg (1999) that computer-mediated modes of communication have emerged from the need to rebuild a sense of community and belonging which is no longer found as people do not share public space as in the past, hence society feels the need to re-establish its former social bonds.

Technical network connections are the main forum for communication in the community and so the community is given structure by the network it has developed within. The infrastructure of the online society is the physical structure of the technology around which it is built as well as the connections, protocols and cyber-space that have allowed it to develop.

The computer underground consists of three deviant groups with some level of social organisation (Meyer, 1989) and a range of other individual deviants and deviant groups (Taylor, 2000) as well as a range of other individual users and groups who do not deviate from the social norms of wider society, including internet hackers and the FOSS community (Jordan and Taylor, 2004). The three organised deviant groups have been identified as ‘pirates’ who are illicit copiers and disseminators of copyrighted software, ‘Hackers’; individuals who engage in illegally entering any computerised system without authorisation and ‘phreaks’ who engage in exploiting the long distance telephone network (Meyer, 1989).

Hackers and phreaks share the same social network (Meyer, 1989; Sterling, 1992); this occurs because they share tools, and are thought to also share ethics. As their activity remains illegal, the computer technology based social network remains the main mode of joining and being socialized into the distinct social forms, behaviour and culture of the group. Jordon and Taylor describe “…a common language and a number of resources by which they can recognise each other” (1998: 769).

Hackers and phreaks tend to frequent the same bulletin boards (BBS’s) and to socially interact with each other (Meyer, 1989), so that although there is some distinction between their activities, there is a shared experience and social interaction. This is a useful grouping as phone phreaking is, in essence, a form of Hack in that the phone line is Hacked. Pirates tend to keep separate from the Hackers and phreaks (Meyer, 1989) as they are more concerned with downloading, uploading and enabling others to share pirated software, rather than the instructional material and unlicensed computer programmes to enable Hacking, which tends to be shared by Hackers and phreaks. Meyer (1989) noted that the boards that are frequented by Hackers and by phone phreaks are transitory in nature and are relatively well hidden from public view.

Hackers will occasionally Hack together, sometimes in the same room at the same time. They hold meetings and conferences, and they use Bulletin Boards, email and Internet Relay Chat (IRC) to communicate with one another. Hackers' biographies have a tendency to include socialization and technical education that involves drawing upon the collective knowledge of the community, as a minimum, this will include accessing online materials, instructions, and resources. More often than not, it includes friendship, mentoring, and tutelage. The computer is seen to be simply a medium for communication, in much the same way that telephony mediates communications. (Sterling, 1992; Quittner and Slatalla, 1995; Jordan and Taylor, 1998). Hackers are not then as isolated as some of the typologies would suggest.

Hackers may Hack in physical solitude, which does not mean we should perceive them as solitary individuals as they will often engage in extensive virtual networks. In all other types of community people spend time alone, and do not come to be seen as any less a part of that community. In fact, many of us now are part of a number of communities, both geographic and virtual (Wenger, 1998). This may include online communities, those that centre on work, friendship, or leisure activities. This means that communities come to be centred on shared practices rather than confined by geographical borders so that the concept of practice comes to be the key defining factor: "The concept of community of practice focuses on what people do together and on the cultural resources they produce in the process" (Wenger 1998: 283).

Jordan (2009) goes on to discuss the need for peer review and education as being essential parts of the being a Hacker, and thus the Hacker who remains secretive and does not share information, or seek to develop his own knowledge and skills is seen to risk exclusion from the hacking community.

The formation of computer-mediated communication has necessitated a reformulation of the ways in which the concept of community is generally understood. Calhoun (1991) suggests that we now frequently engage in what he calls "…indirect social relationships…" in which connectivity with others is transitory and illusory rather than being "real".

> Recent developments have touched issues at the very heart of sociological discourse -the definition of interaction, the nature of social ties, and the scope of experience and reality. Indeed, the developing technologies are creating an expanded social environment that requires amendments and alterations to ways in which we conceptualise social processes.
>
> (Cerulo, 1997: 49)

For Cerulo (1997) there are three key analytic concepts that must be re-examined: social interactions, social bonding, and empirical experience. It is argued by that the apparent nature of online relationships makes it necessary to re-evaluate the need for physical presence as an essential part of the social bonding process.

> Co-presence does not insure intimate interaction among all group members. Consider large-scale social gatherings in which hundreds or thousands of people gather in a location to perform a ritual or celebrate an event. In these instances, participants are able to see the visible manifestation of the group, the physical gathering, yet their ability to make direct, intimate connections with those around them is limited by the sheer magnitude of the assembly.
>
> (Purcell, 1997: 102)

There is also much support for the suggestion that the Hacking community is culturally diverse (Levy, 1984; Hafner and Markoff, 1991; Meyer and Thomas, 1990; Wessels, 1990).

Power and status within the hacking community would appear to be linked to knowledge and trust. It is common practice for hackers to use pseudonyms or ‘handles’ to protect their identity (Levy, 1984; Turkle, 1984; Jordan and Taylor, 1998, Jordan, 1999). They need to build a reputation based upon reliability and knowledge. Status is very important to the level of information-sharing that the individual will have access to. Hackers use Bulletin Boards (BBS’s) as their main platform for communicating with one another along with telephone bridges or loops and voice-mail boxes. Bulletin boards all have authorised users with different levels of access and are connected to other bulletin boards forming a community around the technology; it is common practice for membership of one board to increase the likelihood of access to other boards. Heightened levels of access will also be given to members who can demonstrate that they have extensive social links within the established user group through previous interactions on other boards (Meyer and Thomas, 1990: Jordan and Taylor, 1998).

Hackers have the power to exploit the capabilities of computerised systems, and power over wider society who have a general fear of the unknown threat of new technology and its capabilities (Mordini, 2007).They also have power to manipulate, socialise into community norms and values, or to reject those who are less experienced or less knowledgeable, and so they can be seen to exert power over one another, usually in a hierarchical organisational structure.

Jordan and Taylor (1998) report that Hackers are driven by the thrill of having power over complex and usually inaccessible systems. Jordan (1999, 2009) traces power within cyberspace, and although his analysis is not specific to Hackers but rather attempts to map the entire terrain, it does suggest some interesting and relevant concepts and models, and reveals the hierarchical operation of cyberspace power structures and why and how they operate.

Jordan's (1999, 2009) description of power in cyberspace sees it being operationalised at three levels, the individual, the social and the imaginary; these three levels are perceived to be interlinked as individual and social powers operate within the imaginations of individuals and communities. He calls these the 'powers of cyberspace' and combines the three in formulating his conception of 'cyberpower'.

Jordan (1999) begins with a description of individual power within cyberspace. He suggests that individual power is built up using a combination of identifiers (e.g. handles, e-mail, MUD description) and style; individuals have their own textual style, which is recognizable to people that they interact with frequently. Our identities in Cyberspace are fluid (Turkle, 1997) we may recreate them a number of times in order to operate in different social spaces.

In offline space we also construct identities, but these are constructed in a different way to that in which they are created in cyberspace (Turkle, 1997). We will still find hierarchal social structuring in cyberspace, but the source of identity is text and information rather than being physical or social group characteristics as is usual in wider society. Taylor (2000) suggests that offline hierarchies may be weakened by individual power in cyberspace. Cyberspace at first glance would appear to be anti-hierarchical - allowing equal access to information for all and contributing to reflexivity in late modernity (Beck, 1992) by allowing us to question the authority of expert knowledge. A closer inspection of the social aspect of cyber-power reveals that hierarchies do exist, and that they are based upon ‘techno-power’ - Jordan identifies these as ‘renovated hierarchies’ (2009: 5).

Power is often seen to operate in hierarchical structures. Foucault (1977) rejected this idea; power was viewed as a net, which encompasses all social relationships and is in a constant state of flux and is continually renegotiated within our relationships; although the internet did not exist at the time of writing the metaphorical allusion to a net-like structure is a relevant metaphor for the power networks which have been described as existing in cyberspace. Arquilla and Ronsfeldt (1996) tell us the value of networks as opposed to hierarchical structures, particularly in conflict situations. There is improved capacity due to better communication, better strategic and tactical planning and heightened resistance to attack due to decentralised control and diffuse power. However, within this particular network, the structure soon began to organise itself hierarchically.

When people begin to interact repeatedly or regularly, communities and social groups begin to emerge and to define social norms and values for themselves. This is a decentralized and decentralizing process as the whole collective are involved and no one individual has absolute power. For Jordan (1999) the ability to formulate community is based upon individual power, suggesting a pluralist interpretation of the distribution of power. It is important to note that communities, once formed take on a separate power of their own and so the dialectic between the individual and the community within cyberspace emerges.

In understanding how social hierarchies emerge within the social space created by the internet we must remind ourselves of one simple fact - our level of social engagement is reliant upon our level of technological engagement and therefore our ability to utilize and interact with technology.“ …the communities that provide the basis for virtual individuals are essentially constituted by technologies.” (Jordan, 2002: no pagination) Cyber-power at a social level therefore performs the positive function for society of providing opportunities for shared experiences, and therefore promoting social unity, through the mediated platform of technology. The power, the community, and the technology come to be a singular inseparable unit of analysis.

A difficulty emerges in that ‘techno-power’ is seen to operate in spirals of information overload and information management. Our technologies produce unmanageable amounts of information, so we need to produce management systems for this information, which eventually can be overloaded themselves and requiring further rationalization by the formation of a new system. This can be seen in the emergence and development of the many levels of machine language code - you begin with very simple level language and eventually need to develop a language, which will simplify the previous language. Each stage adds another level of complexity and no single individual person is able to operate in each level of programming. Social power resides in techno-power and social success resides in the ability to manipulate technology. The information needed comes to be more easy to access, but more over-whelming and difficult to use. Jordan tells us that “…the direction of techno-power in cyberspace is toward greater elaboration of technological tools to more people who have less ability to understand the nature of these tools.” (Jordan 1999: 6)

The result is that the:

> …cyberpower of the social is a power of domination, through which members of an elite with expertise in the technologies that create cyberspace increasingly gain freedom of action, while individual users increasingly rely on forms of technology they have less and less chance of controlling. (ibid: 8)

The so-called “cyberpower of the social” (ibid: 8) is rather negative in its outlook, as it suggests the configuration of a controlling and authoritative techno-elite.

This study will show that whilst this may be the case in online communities, and amongst Hackers, it is not the case amongst Ethical Hackers. Please see chapter 5 for a discussion on the social organisation of Ethical Hackers.

Power in the Hacking community and in wider society is seen to be intimately related to knowledge and status, both of which can only be increased in the Hacking community by invitation and acceptance by elite groups. Those with knowledge and status are able to control both positive and negative sanctions on the behaviour of more junior members of the community by restricting or increasing access to information, and also to hacking tools and to privileges.

The reliance of the industry upon hiring Ethical Hackers for designing secure systems and for penetration testing would indicate that it may be possible to apply Jordan’s (1999, 2002, 2009) conceptualisation of a ‘techno-elite’ to an analysis of the status and motivation of the Ethical Hacker. Jordan’s (1999, 2002, 2009) analysis of power in cyberspace suggests that there exists “...an elite with expertise in the technologies”. (1999: 8)

This view is also supported by Thomas (2002), who describes the gulf between the knowledge of the Hacker, and of the everyday computer user; a digital divide:

> As computers become an increasingly ubiquitous part of life and the workplace, the demands for ease of use by consumers as well as demands for high levels of technological sophistication increase. As a result, consumers demand more

> from their technology while understanding it less. That gulf between the end-user and the expertise of the Hackers is growing increasingly wide and provides the greatest threat to security.
>
> (Thomas, 2002: 66)

The imaginary power of cyberspace is seen to reside in its contradictory, potentially utopian, or dystopic, visions of the future (Jordan, 1999; 2009; Mordini, 2007; Winner, 2007). The imaginary also presents a range of potential and should not only be something that is a source of anxiety, but should also be met with a sense of excitement (Mordini, 2007).

> Cyberpower at the imaginary constitutes the broad social order of cyberspace by providing dreams and nightmares through which individuals and communities come to recognize that they are part of something greater than themselves.
>
> (Jordan, 1999: 9)

The individuals and communities are varied and in a state of constant flux. This makes the study of the people and their social organization an important emergent area of study within the social sciences, whilst also making the study complex, difficult and in need of regular review.

The 'imaginary' (Jordan, 1999; 2009) potential of cyberspace has led to fears and anxieties which have created the common misconception of the Hacker as a Criminal, which of course some are, but as we have seen within the typologies that have been created (see section 2.4) many are not. In the following section we will examine the usefulness of traditional criminological theorising in understanding the nature of hacking as an activity.

2.7 Theorising Hacking as Deviance: Criminological Perspectives

Some commentators have suggested that the mass media has been particularly instrumental in the demonization of Hacking and Hacker culture (Pfuhl, 1987; Kane, 1989, Meyer and Thomas, 1990; Kirkpatrick, 2004). In the case of the computer Hacker, a set of anxieties were produced, but these would appear to be disconnected from the actual activity and community of the majority of Hackers (Sterling, 1992; Kovacich, 1999).

The media have used the term 'Hacker' to describe the criminal Hacker, or 'Cracker', as he is known within the community (Taylor, 2000; BCS, 2008; Reynolds, 2003).

> A **cracker** is someone who breaks into someone else's computer system, often on a network; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. A cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or because the challenge is there. Some breaking-and-entering has been done ostensibly to point out weaknesses in a site's security system. The term "cracker" is not to be confused with "Hacker". Hackers generally deplore cracking
>
> (BCS, 2008:8)
>
> Crackers break into other people's networks and systems, deface Web pages, crash computers, spread harmful programs or hateful messages, and write scripts and automatic programs that let other people do these things
>
> (Reynolds, 2003: 60).

The confusion between Hacking and cracking has contributed to the demonization of the activity and the perpetrators; the social anxiety seems to have been projected onto a whole set of related, but much more benign activities (Sterling, 1992). The vast majority of members of the computer underground are not Hackers in the legal sense of the term whereby hacking is perceived to be unauthorized access. Meyer and Thomas (1990) outline the processes through which Hacking came to be demonized through-out the 1980's (Pfuhl, 1987; Kane, 1989), however it must be acknowledged that the creation and growth of cyberspace *has* created new opportunities for social interaction, and therefore new possibilities for committing crime (Capeller, 2001; Williams, 2006; Tavani, 2007, Wall, 2007; 2010; Walden, 2011), and new modes of crime prevention (Wall, 2007; 2010). This new computer mediated networked society means that unauthorised computer intrusion, or Hacking, has increasingly wide importance, as do the entailed modes of prevention.

Commentators have described the opening of a new ‘virtual criminal field’. “The devolution of computer networked access to the domestic arena can be seen as a milestone in cyber-criminal and cyber-deviant activity” (Williams, 2006: 3). The result of this is that:

> Society therefore has no choice but to defend itself against unknown dangers flowing from our technological advancements. We are at war with our with our own products and with our overwhelming technological skills
>
> (Lenk, 1997: 133)

It is also suggested that:

> Criminology has been remiss in its research into the phenomena of cyberspace and has been slow to recognise the importance of cyberspace in changing the nature and scope of offending and victimization
>
> (Jaishankar, 2007: 11)

Jordan (2009) suggests that cracking (access Hacks, or criminal Hacks according to Taylor (2000) and the Computer Misuse Act 1990) can occur in four different ways. There is the original Hack, the modification of an original Hack - which nonetheless requires high level skills, social engineering – either traditional (e.g. trashing) or more recently automated (e.g. phishing), and finally script kidding – which requires very little skill other than the ability to run a programme. By the definitions offered by Wark

(2004) and Himanen (2001), script kidding does not include creativity, and does not offer anything new to society, and therefore is not a pure Hacking activity, but can only be understood as a lower form of imitation. It is included in the typologies, and may also be useful within consideration of communities and power hierarchies as discussed earlier in this chapter, and which will be considered further in Chapter Five.

It has been repeatedly noted that the Hacking community is characterised by a spirit of anarchy, anti-authoritarianism and rebellion (Denning, 1990; Hollinger, 1991; Levy, 1984; Meyer and Thomas, 1990; Sterling, 1992), however it should be recognised that many criminals or deviants act in contravention of, or at the borders of what is socially acceptable, in order to gain a thrill; exhilaration from risk-taking (Lyng, 1990). Entertainment is known to be motivational factor among Hackers (Kilger, 2010). Bachmann (2010) suggested that in his examination of the rationality of hacking that "[p]ersons with a higher risk propensity engaged in significantly more hacking attempts" (Bachmann, 2010: 650). Risk therefore can be understood as a source of positive physiological arousal which is included in the reasoning behaviour of Hackers in choosing courses of action.

Despite acknowledging that there are two types of Hackers, those with good and those with bad intentions, Parker (1998) uses the terms 'Hacker' and 'cyber-criminal' almost interchangeably and lists the following negative and subjective personality characteristics of the Hacker: precociousness, curiosity, persistence, habitual lying, cheating, stealing, and exaggerating, juvenile idealism, hyperactivity, drug, and alcohol abuse.

Criminals have been found to justify their offending behaviour to themselves. It has been suggested that "Delinquency is rendered acceptable to it is perpetrators by justifications” (Jones 2009:146), which means that delinquent behaviour is neutralised through social interactions and cognitive processes which allow the offender or deviant to see their behaviour as ‘normal’.

This is due to the individual needing to feel that the crime that they are committing is not a deviant or ‘bad’ act, as suggested by Sykes and Matza, (1957) who describes a range of strategies for rationalisation of crime. ‘Denial of injury’ (ibid.), as argued from a perpetrators perspective is where the offender believes that no one was harmed by their behaviour (Sykes and Matza, 1957), an example of this is found in the activity of ‘phone-phreaking’ which is an early form of Hacking in which the perpetrator “obtained free telephone calls through the technical manipulation of the telephone system” (Taylor, 2000: 62). The telephone company which lost trade, and therefore revenue, would not have been a cause for concern as they perceived as being able to stand the loss and therefore were not harmed. Sterling (1992) suggests that early phone phreakers had the opinion that the line was just sitting there unused, and that as nothing physical was being taken, then no actual harm was done, and no crime had occurred. ‘Appealing to higher loyalties’ is another technique whereby crime is justifiable to the offender as having a moral basis (Sykes and Matza, 1957). Ethical Hackers (in the underground sense of the word) for example believe in ethics of freedom of access to public information. Through sharing their information they see their actions as a ‘positive activity’ (Wall, 2007: 55), here the concept of ethical utilitarianism is useful in understanding the behaviour as information sharing is seen to be for the good of the whole of society ; In this way hackers who act as hacktivists (e.g. the recent attacks by the hacking groups Lulsec and Anonymous, and also the sharing of information through WikiLeaks) are perceived by some as using the combination of their knowledge and anonymity to benefit the masses. In order to justify the crime the offender will also often shift the blame to another source or circumstance; this is known as ‘denial of responsibility’ (Sykes and Matza, 1957) and suggests that, for example, the Hacker may blame the administrator for not securing their system properly (Sharma, 2007). The ‘denial of the victim’ (Sykes and Matza, 1957) can also be linked to cyber-crime which is non-corporeal crime (true cyber-crime, Wall, 2007), as the victim is not likely to be known to the defendant, therefore if there is no visible victim, the individual may feel there is no harm being done as they have no physical awareness of it and cannot visualise it. The final of these justifications, to ‘condemn the condemners’ suggests that there is dissatisfaction with legal systems and authority holders, (Sykes and Matza, 1957) which is apparent, for example, in the Freedom of Information movement where sharing information is part of the Hacker Ethic as described by Levy (1984), with Hacktivists (Taylor, 2000) and within the FOSS movement.

Gibbs (1993) suggests that this ‘cognitive distortion’ should be understood as being egocentric, and is a psychological defence mechanism, that is designed to protect the individual from the negative feelings that they may feel associated with their deviant or anti-social behaviour. He compliments the above (Sykes and Matza, 1957) with three further cognitive distortions which are blaming others, the attribution of hostile characteristics to others, and the minimising or mislabelling of unacceptable behaviour.

Matza (1964) also believed that young criminals can drift into and out of delinquent behaviour, and that this is actually considered to be normal behaviour for the young, it relates to their stage of social and moral development, and not to they likelihood that they will remain engaged in criminal careers. Young Hackers are often subject to dysfunctional family life (Verton, 2002) which may suggest that the family bonds which can function to reduce the likelihood of offending are not functioning effectively with this group. Matza (1964) successfully combines the concepts of anomie (normlessness), drift and control in his description of the causes of delinquent behaviour. He suggests that adolescents sometimes lack awareness that they are responsible for their actions and so can drift in and out of delinquency. This is because they lack social bonds (Hirschi, 1969) that would increase internal levels of social control.

Steven Box (1971) combines the approaches of Hirschi (1969, bonds of attachment) who stated that *"…*delinquent acts result when the individuals bonds to society are broken" (1969:16) and Matza (drift theory, 1964) to produce a list of variables which he said must be considered; the likelihood of offending was thought to be significantly increased by the presence of each. These are:

1. Secrecy
2. Skills
3. Supply
4. Social support
5. Symbolic support

This is relevant to an understanding of cyber-crime as each of these is increased by or offered by membership of the Hacking Underground. This offers an alternative for those with weak bonds to mainstream society, who may therefore become more bonded to the subcultures that are offered within the communities of cyberspace.

As described earlier in this chapter Hackers frequently work as part of a group, or will act as part of a network or community, sharing new ideas and links with each other; in many cases this allows them to show off their work and what they were able to achieve. Cohen (1955) suggests subculture forms from the 'problem of adjustment' which is that an individual has failed at a previous task or does not perceive there to be sufficient value in their status within society which then leads to 'reaction formation', an idea which developed from Freud where that individual then joins a group of people in the same situation as themselves. These individuals then undertake delinquent behaviour to gain status within the group. This can be done by Hackers who will gather on forums to share information, and brag about their exploits, as a means of gaining status.

Cohen (1955) said that the delinquent groups form from working class boys who struggle to achieve status. Typologies would suggest that gaining status through the Underground Hacking community is also a male behaviour, but access to the technology has meant that the technology was first accessible to wealthier middle class boys, and that this later spread to the working class. Status and success in the community is linked to knowledge and skill rather than to wealth or to the possession of material goods.

Hirschi (1969) suggests that there are four factors which can reduce the likelihood of a crime occurring which were attachment, commitment, involvement and belief; the extent to which these factors are found to be present, is inversely proportional to the likelihood of a criminal event .

The anonymous environment would make a person more likely to commit a crime online as they are aware that they are less likely to be caught and prosecuted (Jewkes, 2003; Jaishankar, 2009; Rege, 2009). This is important in considering strategies of encouraging and supporting desistance. In young cyber-criminals increasing the attachment to, commitment to and involvement in wider society, as well as increasing the belief that the rules of wider society should be adhered to will reduce the likelihood of criminal activity.

Hirschi's control theory (1969) further suggests that people follow the law as they are rational decision makers and that they will weigh the cost of committing the crime with the outcome of the crime to decide whether or not to carry out a crime (Toby, 1957). Hirschi (1969) suggested that law breaking was a natural behaviour shown by some humans, he attempted to understand why some people committed crimes and others did not and found that this was rational process that was influenced by the level of formal and informal social controls. As we have seen in the previous section, the current legal framework, and the very low likelihood of prosecution reduce the impact that may have been had by these formal mechanisms. Informal modes of control, as we shall see in Chapter Five, do seem to have had some impact on the decision not to engage in criminal Hacking, but rather to find a legitimate use for these skills. Therefore Control Theory is only partially useful in explaining this activity.

A person who commits crime online is far less likely to commit a crime in the real world due to the guilt that they would feel for others around them, suggesting that when committing cyber-crime they do not recognise that there is a victim (Sharma, 2002). This was found to be the case in the infamous 'rape in cyberspace' committed in the multi-user domain LambdaMOO by Mr Bungle, who was in real life a group of college boys who engaged in the act for fun (Dibbell, 1998). Brenner (2002; 2004) suggests that criminals take part in online delinquent behaviour due to the anonymity and non-corporeality resulting in a lack of costs in the form of prosecution and therefore a lack of deterrence, resulting in cyber-crime (Jaishankar, 2009; Jewkes, 2003, Rege, 2009); this again relates to control theory as there is a lack of formal social control online. There are clear informal controls within the computer underground, but as we have seen these can value illicitness and therefore actually serve to encourage behaviour that deviates from the wider population, despite being acceptable to, and encouraged by certain factions of the computer underground.

Crime as also seen as a form of testing boundaries, as risk taking that is thrilling. Even though there are high costs involved, the aim is to gain the thrill and the excitement, without the associated costs. This suggests that ‘edgework’ may be a useful concept (Lyng, 1990). Committing deviant acts as a way of gaining emotional satisfaction is recognised within cultural criminal because, “While we cannot make sense of crime without analysing structures of inequality, we cannot make sense of crime by only analysing these structures either” (Ferrell, 1992: 118-119). As previously discussed, gender would appear to be important in that Hacking seems to be a male activity, but socio-economic status has little bearing. Analysing structures of inequality, while a popular pursuit in mainstream criminality, has little use in this analysis.

“Rational Choice Theory holds that people are rational and weigh up the potential costs and benefits of committing crime” (McQuade, 2006: 144). Rational Choice Theory sees everyone as a potential offender, but suggests that the circumstance that the person is in is an important factor in deciding whether or not they will commit a crime. Individuals will use a cost-benefit analysis to weigh up the potential positive and negative outcomes of committing a crime in order to decide whether or not it is actually worthwhile committing the crime (Clarke and Cornish, 1985; Cornish and Clarke, 1986). Cornish and Clarke (1986, 2008) suggested that there were a number of significant factors involved in this calculation and that these comprise of, effort involved, the perceived risks, and the level of anticipated rewards. Rational Choice Theory can be applied to cyber-crime because “Goals or benefits of committing crime may include acquiring money or other goods and services, exacting revenge, gaining recognition, becoming thrilled…thrill seeking is a common motivation of Hackers" (McQuade, 2006: 144). Other motivations are explored in the section that follows.

Cornish and Clarke (1986, 2008) suggested that a series of choices must be made, and that social and psychological factors influence these choices. Crimes would be committed by the offender with the intention of gaining some positive desired outcome, whilst avoiding pain, or punishment (Higgins, 2007). Ferrell (cited in Sharma, 2007:14) describes it as the "…exhilarating, momentary integration of danger, risk and skill" which motivates a person towards criminal behaviour. Grabowsky (cited in Sharma, 2007:14) believes that of Hacking is "an act of power… gratifying in and of itself" and that the Hacker is intrigued by the "exploration of unknown".

It is believed that most computer Hackers are young men who are extremely intellectual and motivated; as previously discussed, some theorists also suggest that Hackers tend to lack social skills (Hollinger, 1991; Post, 1996; Boni and Kovacich, 1999: Lilley, 2002a). Hacking is therefore seen as being a form of entertainment and a social activity for these 'outcasts' , and as we have discussed, where the chance of being caught and prosecuted if they do commit crime is considerably reduced, and therefore deterrence is minimal (Jaishankar, 2009; Sharma, 2007). "Hacking produces rewards and seduces the youth and the lack of internal controls in form of ethical standards facilitates the commission" (Sharma, 2007:18). It has frequently been noted that hacking is thrilling and exhilarating, and that many engage in it for fun or entertainment (Kilger, 2010; Stouffer *et al.* 2011).This is suggestive that Cultural Criminology may be of use in understanding the nature of criminal hacking, but also clearly indicates that there is a rational element to hacking, whereby a reasoning process occurs, albeit a bounded reasoning, in that Sharma indicates a lack of ethical standards. This could be due to a lack of knowledge and understanding of normative and meta-ethical approaches.

It is apparent that a range of traditional criminological theory can be applied to different types of Hacking behaviour; however, these have not been applied to Hacking which is not defined as deviant or criminal despite the activities engaged in being similar.

The diversity of Hacking activities and Hacker types mean that a wide range of criminological theory is applicable to Hacking, but that different theories are useful for different types of Hacking activity, with no one theory being comprehensive in its ability to fully explain all types of Hacking behaviour.

In chapter 5 a model for understanding Ethical Hacking behaviour is proposed which makes use of some elements of Rational Choice Theory; in order to fully understand the behaviour it is necessary to adapt the theory, making use of economic bounded models of rationality. Please see section 5.2 for a full discussion.

The following section will discuss the emergence of Ethical Hacking which arises as a response to the way in which computing, the internet and hacking have developed.

2.8 The Emergence of Ethical Hacking

Despite the apparent diversity, the network of social support, the freedom and the hedonism offered by having membership of the Hacking community, it is the case that a number of Hackers choose to come to be contracted by, or co-opted into, large corporate entities or the security industry. Many have commentated that motivations and ethics have remained the same among the Hacking community, even though the activities have diversified in response to the development of technology (Felsenstein, 1992; Meyer, 1989; Sterling, 1992).

The Hacker who chooses to ‘cross the line’ and come to be a legally sanctioned Hacker on behalf of the computer security industry has been categorized as the ‘Ethical Hacker’ by academia (BCS, 2008). There is less willingness to accept the term from within the Hacking community. The term “techno-yuppy” has been widely utilized online to describe the self-employed Ethical Hacker; the term “microserf” (Taylor, 1998) has been used for those who enter employment by software and telecoms industries, and then utilise the techniques, data and systems they have access to for their own personal Hacking purposes. As will be discussed later in this chapter these Hackers change their behaviour because their external or offline social relationships and motivations change with age, in common with other forms of crime and deviance; aging changes the relative values associated with the costs and benefits of their behaviours.

“A market …exists for what is known as “ethical hacking”, whereby hacking skills and methods are applied against a system by persons who can be trusted not to use any of the discovered weaknesses for illegitimate purposes” (Furnell, 2002: 231)

Kimberley Graves (2007) suggests that “Ethical Hackers usually fall into the white-hat category, but sometimes they’re former gray hats who have come to be security professionals and who use their skills in an ethical manner.”

This study commenced with the assumption that the majority of Ethical Hackers had underground origins. On closer examination it has quickly became apparent that the Ethical Hackers who learn their skills underground and have underground beginnings and affiliations now only make up approximately half of Ethical Hackers and that this is declining (according to the respondents in this study); those with criminal records make up only a small percentage and are becoming increasingly rare, for reasons that are fully explored later in this section. The other category which emerged were those who had moved into a knowledge of Hacking from legal, security, or marketing backgrounds, and who self-reported that they had never and would never engage in any illegal Hacking activities, although they utilised the same skills and knowledge as Hackers in the course of their employment.

The aim of Ethical Hacking behaviour is defined as being "…to help the organization take pre-emptive measures against malicious attacks by attacking the system himself; all the while staying within legal limits" (www.eccouncil.org/CEH.htm, no date).

According to the British Computer Society (BCS):

> An Ethical Hacker is a computer and network expert who attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious Hacker could exploit. To test a security system, Ethical Hackers use the same methods as their less principled counterparts, but report problems instead of taking advantage of them.
>
> (BCS, 2008:7 http://www.bcs.org/upload/pdf/ethical-Hacking.pdf)

As we will see later in this chapter, the British Computer Society separately rejects the academic understanding of the Ethical Hacker as someone who is employed and therefore sanctioned, which they seem to accept in the above description. They criticise its use in the title and marketing materials for programmes of study.

By this definition, the only distinction that is perceived to exist between the Hacker and the Ethical Hacker is the legal distinction, which sees Hacking in terms of unauthorised access rather than the motivations which underlie it or the processes that are employed.

The role of the Ethical Hacker has come to be essential across business, commerce, government, academia and other large organizations with complex information systems, and confidential data to protect. As we will discuss within this chapter, the computer security industry is perceived to be undergoing a period of rapid growth, and therefore offering good career opportunities, good pay and job security for the Ethical Hacker. The increased functionality and use of the Hacker within the security industry has led to a need for 'Ethical Hacking' qualifications, the most well known of which is the 'Certified Ethical Hacker' (CEH) provided by the International Council of E-Commerce Consultants.

It has been suggested that employed Ethical Hackers should be beyond the peak age identified for Hacking activity which would reduce the associated level of risk:

> ...by the time they were 30, there was a transformation. In fact, most of them were interested in a career. It took them till [that age] to become emotionally mature. Just a small minority would be dangerous, but the vast majority would be of extreme positive use to society.
>
> (Schell, 2004, www.bbc.co.uk).

This would imply that Ethical Hackers go through some personal change or maturation, which causes them to alter or re-order their own personal goals and values. Perhaps there is a process of desistance from offending and deviance, which is similar to that identified among offenders more generally and is associated with education, employment and families (Soothill, et al. 2009). Hirschi (1969) would identify these as providing a set of informal controls which reduce the likelihood of offending. Control theory starts from the assumption that people will commit crime if they can, because it is profitable, useful or enjoyable. They have a lack of internal control so they need to be externally controlled through informal and formal modes of control. As we will see in the later discussion on the law, formal controls are not as effective, being only adhered to by Ethical Hackers through choice. For this reason it is necessary that individual's informal controls instil them with a sense of respect for the formal.

Desistance from offending is often not complete, but can more accurately be described as being 'curved' (Leibrich, 2003). Rather than complete desistence, Hackers will reduce their offending, or reduce the harms associated with their offending. They will engage in Ethical hacking, but will often continue to engage in illegal activity despite apparently 'going straight' (Please see chapter 5).

Stefania Ducci of the Hacker Profiling Project (Chiesa and Ducci, ongoing) was interviewed about the research by Federico Biancuzzi on November the third, 2006. She states that:

> It emerged from the questionnaires that so-called "Ethical Hackers" inform sysadmins of vulnerabilities on violated systems (or contribute to fix security flaws), but usually only after having informed other members of the underground. It came out also that they do not crash systems (if this happen it is accidental and due to inexperience), and neither steal nor delete nor modify data. Their aim is to improve the systems' security and raise sysadmins' awareness and attention.
>
> (http://www.linux.com/archive/feed/58137, 2006)

This perception of the Ethical Hacker is quite different to the definitions that are employed within academia; it focuses more upon questions of morality and ethics than upon legality or authorisation, and therefore it relates more to the underground understanding of the term than it does to the now generally accepted industry and academic use.

Ethical Hackers, for the purposes of this research, are defined as being those individuals who utilise skills and knowledge used by Hackers, whose personal journey has resulted in them becoming either contracted or salaried by various organisations with the aim of providing, or tightening security against the Hacker. They work towards reducing the impact of Hacking or other cyber-crime for a particular business or organisational interest, whether their original roots were in 'white hat' or 'black hat' Hacking, and whether or not they engage in any Hacking activities outside of their employment.

2.9 Conclusion

Jordan (2009) suggests that any formulation of a definition of Hacking must include the popular conception that it is an activity which relates to computing and networked technologies. To combine what Himanen (2001), Wark (2004) and Jordan (2009) suggest, Hacking is making a difference, either to advance society or technology, by using or altering computing or networks. When we take this idea about the nature of Hacking and consider it in combination with the classic research and scholarly approaches to what Hacking is (Taylor, 1999; Turkle, 1984; Hollinger, 1991; and Thomas, 2002) we must add the commonly agreed idea that Hackers are drawn to transgressing legal or societal conventions, and so we must add illicitness (Turkle, 1984) and therefore deviance to this emerging description.

Late modernity has produced a general shift in society towards an obsessive need to categorise, understand and explain (Beck, 1992). The Hacker is a phenomenon that has been subject to such categorisation as illustrated in the typologies provided above; Hacking has come to be seen as a risk, an uncontrollable danger due to our fears of that which we fail to understand. This fear has been amplified due to the ways in which the media has played upon these fears in order to reconstruct the term to have a much more negative and fearful set of connotations to those that were apparent when the term was first used. As Beck (ibid) notes, increased levels of risk increase the reliance upon experts, hence the Hacker creates the need for the Ethical Hacker, in order to control the created level of risk.

The development of Hacking, along with a late modern reflexivity and heightened awareness of risk, and reliance upon experts (Beck, 1992) has created the need for the so called ‘Ethical Hacker’, this group is a social and an academic construct, and defines a group who are different in nature, motivation and characteristics to both crackers and internet Hackers, yet who share the skills and abilities of the Hacker, if not the same community and ideology.

The context provided here will be important to understanding the Ethical Hacker who as emerged as a recent development in the history of Hacking; the history of the Hacker is therefore the history of the Ethical Hacker.

Chapter 3: Regulation for Cyberspace: Ethics, Morality and the Law

3.1 Introduction

It has been questioned whether it is really necessary to develop a new set of regulations for cyberspace, when current ethical and normative systems may suffice (Easterbrook, 1996) however, despite the objections, Maner (2004) is emphatic that this regulation is necessary, and he also explains why he believes this to be the case; it is suggested that there are a range of new issues which did not, and could not have previously existed. These issues relate to the scope and the scale of cyberspace and to the new opportunities that these created whereby the scope and the scale of the deviant activity and its associated harms are also increased (Wall, 2010; Tavani, 2007). As discussed in Chapter Two, cyberspace creates a range of possibilities for both new behaviours, and also for new modalities of control. Cyberspace has exaggerated previous issues, e.g. invasion of privacy or the dissemination of harmful information, it has converted previously existing issues such as espionage, theft, fraud, stalking, sabotage into larger scale events that have more harmful outcomes which can be commissioned more effectively with less risk of being caught, and cyberspace has also created completely new opportunities, as is the case with computer Hacking (Stamatellos, 2011). Computers are seen as being malleable in their logic in that they can be adapted to a number of purposes; they are therefore able to afford us with wide-ranging new opportunities (Jordan, 1999, 2008) including opportunities for general creativity (Moor, 1985), together with creativity in criminal practice, crime prevention and detection of crime.

These new and old opportunities, and exaggerated outcomes have led to a number of legislative issues which will be explored in the following section.

The chapter will then go on to consider alternative social controls and how these apply in cyberspace, including the use of code to control the architecture of cyberspace, and the impacts of morality and ethics upon behaviour among underground Hackers. This will provide the context for analysis of Ethical Hackers decisions about ‘right’ and ‘wrong’ behaviour, which can be found within chapter 6.

3.2 Computer Misuse: Legal Remedies

If Hacking is to be defined as a criminal activity, it must be understood in relation the development of the legal framework which outlaws it.

There are three main areas of computer misuse related crime which need to be considered in the light of the possible legal remedies; these are traditional crimes, content related crimes, and integrity related crimes (Wall, 2007; Walden, 2011), these will be defined and discussed in the section that follow. Remedies for computer misuse can include the use of existing laws and statutes, the amendment of existing laws and statutes and the creation of completely new and specifically designed laws and statutes. It is possible to also consider which remedy is the most applicable in the view of the three approaches outlined above by Stamatellos (2011) with regard to whether offences committed are an exaggeration or conversion of a traditional form of crime, in which case it may be possible to use existing or amended legislation, or whether they constitute the creation of a new offence and therefore requiring new legislation or the amendment of existing legislation.

3.2.1 Traditional Crimes

Walden (2011) begins his account of the possible legislative responses to cybercrime and the rationales behind them by discussing traditional crimes. These are crimes which can also occur without the use of a computer; as we have seen it may be applicable to use existing statute in dealing with crimes which are already extant (Easterbrook, 1996). It could however be argued using Stamatellos' (2011) formulation that that the scope and the scale of traditional crime has been sufficiently increased by the use of computers to necessitate amendment or new statute. An example of this exaggeration of range and extent can be seen with reference to privacy and confidentiality issues, where the spread of data can be much more extensive using networked technology and therefore exaggerating the threats posed. This would be seen as the transformation of traditional crime, where the crime is the same, but its impact can be greatly increased because of the use of new methods and new technology. As traditional crimes are exaggerated or converted in these ways, Walden (2011) examines in detail the applicability of existing statute, and also considers the impact and the effectiveness of some of the amendments which have been made.

Traditional crimes which are "computer related" or which employ the "computer as instrument" (Walden, 2011:554) are specifically examined. There are three main areas of traditional crime that are included within the discussion, these are: theft of information, fraud, and forgery, and these three will now be considered in depth.

Theft of information, according to Walden (2011) may occur for many reasons, including thefts for political or financial reasons. It is generally carried out by, or against, states, political organisations, or financial competitors. The theft will be carried out by either insiders within an organisation or will be an external threat; each posing a different level of risk, and different means of prevention. An insider attack can be defined as being "…the intentional misuse of computer systems by users who are authorized to access those systems and networks" (Schultz and Shumway, 2001: 256). These attacks are carried out by "…employees, contractors and consultants, temporary helpers, and even personnel from third-party business partners and their contractors, consultants, and so forth" (Schultz, 2002: 527), but Pfleeger (2008) also includes within the definition "a former insider, now using previously conferred access credentials not revoked when the insider status ended or using access credentials secretly created while an insider to give access later" (Pfleeger, 2008: 6), so that previous insiders become outsiders but often retain their access privileges. This type of computer misuse is mainly carried out by the 'Industrial Hacker' and the 'State Sponsored Hacker' according to the typologies in the Hacker Profiling Project (Chiesa and Ducci, 2008) as discussed in Chapter Two.

The theft of information by computer Hackers often does not fit neatly into this formulation because a number of computer Hackers are neither politically nor financially motivated, but rather are motivated by the curiosity, the desire to explore and the challenge of accessing information (Denning, 1990; Stouffer et al, 2011), and will therefore steal or copy information to use as a trophy, as evidence of their prowess and not simply for the possession of the information itself, or to damage it, or pass it on to others. Although the crime may appear to be the same, the motivation is often very different.

Denning (1990) concurs with this view, describing Hackers as being people who are curious and who have a desire to explore, but she also suggests that they generally wish to use the knowledge that they have gained for the benefit of others, and wider society, in line with the Hacker Ethic as was described by Levy (1984). This utilitarian approach to decisions and behaviour will be considered in full within Chapter Six with reference to the specific behaviour and decisions of the respondents to this study, and their perceptions of the industry as a whole.

Theft of information may be carried out by Hacking or by eavesdropping, and the computer itself may be either the means of accessing the data, or may be the means of data storage, often using hard drives or USB memory devices (Walden, 2011). More recently, in an increasingly networked environment, it is becoming more common to use hijacked servers for data storage. Respondents with affiliations to the underground tended to see this as not being problematic, despite it being a clear infliction of the legal code. Although illegal, this is generally fairly benign behaviour, typically involving data storage or sharing of media files. A full examination of the responses of the participants in relation to this issue is also to be found within Chapter Six.

The copying of data does not constitute a theft in the traditional sense of the word as section 1 of The Theft Act of 1968 specifically defines that "…a person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it" (Great Britain, The Theft Act 1968). Traditional theft laws have proven to be inapplicable as they include the requirement that the intention of the perpetrator is to 'permanently deprive' the owner of their possession. The copying of data does not therefore meet the specifications of the Theft Act 1968 due to the fact that a copy is left for the owner and therefore the owner is consequently not deprived of their possession.

Section 15 of the Theft Act 1968 goes on to discuss the offence of fraud, which Walden (2011) also suggests is a major area of legal concern within what he categorises as ‘traditional crime’. Legislative consideration was required since the crime of fraud increasingly had become computer related, or otherwise utilised the computer as an instrument in the commission of the fraud. Fraud is here defined as being committed by “...any person, who by any deception, dishonestly obtains property of another with the intention of permanently depriving the other of it.” (Great Britain, The Theft Act 1968). Fraud is therefore a form of theft, but requiring a deception to have occurred as part of the commissioning of the offence. Problems have arisen in that case law (e.g. Thompson [1984] All ER 565) has dictated that the deception should be of a person rather than of a computer or of a network. Deception is specifically defined as being “To induce a man to believe a thing which is false and which the person practicing the deceit knows or believes to be false.” (Great Britain, The Theft Act 1968)

This and other lacunae led to the creation of three new offences under the Fraud Act 2006. These are:

a) Fraud by false representation
b) Fraud by failing to disclose information
c) Fraud by abuse of position

Section a) being specifically designed to include fraud against or making use of a machine.

It is also the case that existing laws have not been applicable in all cases of forgery and counterfeiting, with the now infamous case of R V Gold and Schifreen being instrumental in necessitating the formulation of the Computer Misuse Act (CMA) 1990. Lord Lane described attempts at applying existing statute in the shape of the Forgery and Counterfeiting Act of 1981 to the case as "Absurd" ([1997] WLR 803 Lord Lane CJ at 8095). Gold and Schifreen had been prosecuted at Southwark Crown Court after they had accessed BT's Prestel System for email, and in particular accessed the Duke of Edinburgh's own personal email account. They were both charged under the 1981 Forgery and Counterfeiting Act and they were initially convicted, however a later appeal was upheld due to the fact that the "false instrument" and the "deceived" were found to be the same object; the "deceived" is generally expected to be a person which meant that there was no applicable case law to provide a precedent for prosecution. Section 1 of the Act states that "…a person is guilty of forgery if he makes a false instrument with the intention that he or another shall use it to induce *somebody* to accept it as genuine." (Great Britain, The Forgery and Counterfeiting Act 1981) with the clear implication the 'induced' must be a person.

Traditional crimes have proven difficult to prosecute when they have been committed using computers. This is suggestive of the need for specific legislation relating to computer misuse, even in the case of traditional crimes. The introduction of this legislation and its success is discussed in section 3.3.1.

3.2.2 Content Related Computer Misuse

The second area of computer misuse discussed by Walden (2011) considers content related crimes where the computer is used as an instrument, and where the content is itself also illegal. The discussion from Walden (2011) relates specifically to the possession and supply of child pornography however Wall (2007) uses a wider definition and suggests that Computer content crimes are crimes which are "…related to illegal content on networked computer systems and include the trade and distribution of pornographic material as well as the dissemination of hate crime materials" (2011: 50).

While child pornography and its creation and dissemination is largely irrelevant to a discussion on Hacking, the ways in which downloading, caching, altering and storing data came to be viewed by the law as a result of precedents set may be useful in understanding issues surrounding creating and disseminating Hacker tools.

These computer related crimes where the computer is used as an instrument have meant the conversion of existing types of crime (as is the case with pornographic material) and also the creation of new crimes (Hacker tools) and have largely been dealt with through the amendment of existing statute.

The supply of child pornography was covered by the Protection of Children Act of 1978 which made it an offence to take, or permit another to take 'indecent' photographs of children, and also to "…distribute, publish, show, or possess with the intention to distribute…" (Great Britain, Protection of Children Act of 1978). The Act outlawed the making of indecent material of children, with the act of making viewed in law as being an act of supply. It was not until the Criminal Justice Act 1988 that it became an offence to own an indecent photograph of a child. The Criminal Justice and Public Order Act 1994 extended the powers of the Criminal Justice Act 1988 and the Protection of Children Act 1978, and was designed to cover 'artificial' child pornography – pseudo-photographs and digitally generated images, even where the image is of a consenting adult, if they are portrayed as a child. This illustrates the need for laws to develop inline with advancements in technology. The definition of photograph is also extended to "…data stored on a computer-disc or by other electronic means" (Great Britain, Criminal Justice and Public Order Act 1994) in order to reflect the way photographs are now stored and to close this 'loophole' by clearly defining what is meant by the terms within the law. As we will see later in this chapter, attempts to clearly define the meaning of the terms employed within the Computer Misuse Act (1990) and also within the Police and Justice Act 2006 have been resisted in order to allow the requisite flexibility in case of further technological advancements.

Issues arising from case law with regard to computers as instruments have led to definitions regarding possession, making and supply being more clearly redefined. In the case of Jayson [2002] EWCA Crim 683 it was held that downloading constituted an act of making, and therefore was perceived under the law as an act of supply. If was ruled that a download would be considered an act of making even where the download was not stored due to the functionality of the 'cache' memory, which automatically carries out the act of making. This was further clarified in Atkins and Goodland V Director of Public Prosecutions [2002] All ER 425 in which it was decided that the court would have to prove that the defendant was aware of the cache memory and how it functioned. In the case of Jayson the cache had in fact been altered and therefore it was clear that the defendant was aware of the cache and the functionality of it. This has clear implications for those who download hacking tools, even if they have not made, used or distributed them. In order to be prosecuted, they simply need to possess them, and to know how to use them.

3.2.3 Integrity Related Computer Misuse

The third of Walden's (2011) areas of computer misuse for consideration are crimes which pertain to the integrity of computer data. Walden identifies these as "…offences which attack the integrity, confidentiality and availability of computers and communication systems." (2011: 554). According to Wall (2007: 49) "Computer integrity crimes assault the security of network access mechanisms". These crimes have been dealt with using the creation of completely new statute and also by the amendment of existing statute. Using Stamatellos (2011) analysis as a framework would lead us to identify the transformation or 'conversion' of traditional forms of crime in the access to and damaging of information and would also point to Denial of Service (DoS) attacks as new crimes requiring new statute. A DoS attack is where the functionality of a computer, site or network is impaired, and this can be by either authorised or unauthorised traffic. DoS attacks that were commissioned with an excess of authorised web traffic were not prosecutable under the Computer Misuse Act of 1990. New statute that would be able successfully deal with a DoS attack was not enacted until 2006 when the Police and Justice Act amended the Computer Misuse Act of 1990.

Examples of crimes within this category include gaining unauthorised access, particularly with the intent to commit further offences, unauthorised acts including criminal damage and the use of "unlawful devices" such as password, codes or usernames to which the user has no entitlement or systems which enable the user to bypass such security measures.

3.3 The Development of UK Legislation against Computer Misuse

As we have seen, traditional crimes, content related computer misuse, and integrity related computer misuse (Walden, 2011) have raised a variety of issues requiring the formulation of new legislation to control computer misuse. The Computer Misuse Act was initially introduced in 1990 in response to a number of cases which could not be dealt with under existing statute and following on from similar legislation in the US. The legislation has been subject to a number of suggested and actual revisions. This development of the UK legislation and the extent to which it can be considered successful or effective will be outlined in the following sections.

3.3.1 The Computer Misuse Act (CMA) 1990

The Act was introduced through a Private Members Bill on 29 August 1990. It was designed to "make provision for securing computer material against unauthorised access or modification". The Act is separated into three sections:

1. Unauthorised access to computer material
2. Unauthorised access with the intent to commit or facilitate the commission of further offences
3. Unauthorised modification of computer material

(Great Britain, The Computer Misuse Act 1990)

In 1995, 26 year old Christopher Pile was prosecuted under the CMA (1990) for disseminating viruses "Pathogen" and "Queeg" and was subsequently sentenced to eighteen months imprisonment for five counts each under sections one and three of the Act (R V PILE).

“The CMA suffered a premature birth which left it weak and vulnerable when the internet, as we know it, arrived” (MacEwan, 2008: 1). It has been asserted that the CMA was hastily prepared, not comprehensive in its coverage of computer misuse, and ill prepared for the changes in computer technology which were to come in the next decade and in particular for the mainstreaming of network technology (MacEwan, 2008).

The CMA saw fewer than 10 prosecutions in its first decade. It did not, at its inception, include Denial of Service attacks (DoS) as these do not require access and only makes authorised modifications.

A DoS attack occurs:

> When a deliberate attempt is made to stop a machine from performing its usual activities by having another computer create large volumes of specious traffic. The traffic may be valid requests made in an overwhelming volume or specially created protocol fragments that cause the serving machine to tie up significant resources to no useful purpose.
>
> (APIG, 2004)

The terms “data”, “programme” and “computer” were not initially defined for fear that definitions might rapidly come to be obsolete. In DPP V McKeown; DPP V Jones (DPP v McKeown; DPP v Jones [1997] 1WLR 295 (HL)) Lord Hoffman defines the computer as being “a device for storing, processing and retrieving information”. This is, at best vague and ambiguous, however APIG (2004) comment that the ambiguity is positive, has not caused any issues and allows courts the freedom to apply the current contemporary understanding of the term, so that such attempts to define should be avoided.

A major social issue which had been raised with the original Computer Misuse Act 1990 (unamended) was the criminalization of unauthorised access. Unauthorised access has been likened to trespass, which is in fact a 'tort' in the UK; it is a civil rather than a criminal offence. The appropriateness of treating computer misuse differently to other forms of trespass is questionable, particularly in view of the fact that in the UK there is no general right to privacy that is protected in law. Also, words and information do not have the same legal status as property. Criminalization labels a whole generation of Hackers who had been previously engaged in perfectly legitimate activities. This causes the need for some to find ways to continue with the same activities, but without circumventing the law. This may partially account for the rise in Ethical Hacking.

Another area of the Computer Misuse Act 1990 which has been brought into question is that in order for an offence to have taken place, access or modification must have been unauthorised. The case of DPP V Bignell [1998] 1 Cr App R8, illustrated the difficulties which can arise. The Bignells were serving police officers who had requested confidential data to which they had authorised access; the access was for personal rather than professional purposes. The issue identified by this case revolved around the inability of the Divisional Court to differentiate between illegal access to information and misuse of information. The House of Lords later criticised the Divisional Court for failing to focus on the real issue, which was the authority to access the actual data, rather than the type of data. Wasik (2008) describes this as being inconvenient and inviting criticism. He suggests that access being granted for one purpose cannot be seen to imply access for any other purposes. This reveals a loophole in the application of the act, rather than a failing in the actual Act itself. The

Law Commission in 1989 had stated that even though the CMA was aimed at the remote Hacker, it was however “apt to cover the employee or insider as well” (Law Commission, 1989: para 3.35).

Another example of a loophole occurring in the application of the Act occurred in the Bedworth case which caused there to be calls for amendments to the Computer Misuse Act 1990. As the first case to be tried under the Act, the acquittal of teenager Paul Bedworth, after a sixteen day trial at Southwark Crown Court caused a media sensation as well as questions to be raised about victim precipitation and in particular, debated about offender culpability in the light of victim precipitation. The Bedworth case, as with the Gold and Schifreen case before it, has come to be known as a ‘Hacker’s charter’ in that it set an important legal precedent. Bedworth had, it was claimed, interfered with Allied planning for the Gulf war. As a teenager with a £200 computer, it was questioned whether this should even have been possible and whether in fact the ‘victim’ should take some responsibility for failing in their duty to protect their digital property, particularly given its importance to national security. Bedworth’s acquittal was on the grounds that he did not have the sufficient intent for conviction, in that he was addicted to Hacking as an activity and that he had not set out to do any harm.

The crime that is not recorded in police statistics because it is either unknown to the victim, is unreported by the victim, or unrecorded by the police has long been termed ‘the dark figure of crime’; it is therefore an unknown quantity. Computer misuse is thought to have a massive dark figure for several reasons; the victim may not be aware that they have been victimised, they may think that the police are unlikely to prosecute, based upon the above, or the police may decide that progressing the investigation is not financially worthwhile, or that it will be too difficult to secure a prosecution. One of the police officers interviewed for this research described how many minor cyber-crimes would not be taken further by the police as they did not have the resources available. The so-called dark figure has a major impact when evaluating the usefulness of any legislation; crimes which are not reported or recorded, cannot be dealt with under the law, and their extent is unknown. We cannot know how successful the legislation is, because we cannot accurately know how much cyber-crime there is.

Bachmann describes the problem:

> The ongoing uncertainty of punishment is particularly problematic because it severely undermines any efforts to deter criminal behavior in cyberspace. Indeed the high risk awareness that appears to be rooted in rational decision making processes suggests that many hackers are aware of the current improbability of becoming detected and prosecuted.
>
> (Bachmann, 2010: 653)

Rational Choice Theory would see us as reasoning, rational beings that make our choices by weighing up potential outcomes in terms of costs or limitations, against possible benefits or gains (Clarke and Cornish, 1985; Cornish and Clarke, 1986; Cornish and Clarke, 2008). This type of analysis will lead many victims of crime, if they are even aware that they have been victimised, to choose not to report the crime as the potential costs can be very high, with very few associated gains.

There is a clear risk to businesses of further losses being incurred if the crime is reported, both in legal costs, and also in loss of reputation and associated loss of trade, leading to further economic losses. Please see also Chapter Six for a full examination of the respondent’s views on the law and how it affects their decisions and behaviour.

The Computer Misuse Act (CMA) of 1990 makes the act of computer misuse a criminal rather than a civil offence, meaning that there is no associated entitlement to either restitution or compensation for victims of cyber-crime under the Act. The lack of evidence, limited reliability of evidence and the difficulty in policing also mean that successful prosecutions are not likely. From 1990 to 2006 only 214 defendants were tried for Computer Misuse (APIG, 2004). This has led to a questioning of the usefulness of the Computer Misuse Act 1990 as a deterrent. Although the conviction rate of defendants is relatively high, most crimes are not brought before the courts. This may impact upon the cost benefit analyses that are carried out by individuals engaging in cybercrime. The low associated costs would do little to deter the potential offender.

Revisions to the Computer Misuse Act of 1990 in the 2006 Police and Justice Act would also include the criminalization of the creation, possession and supply of Hacking tools. These are not included in Walden's (2011) discussion outlined in the previous sections but will be further reviewed in the following section in relation to the process of amending the CMA 1990.

3.3.2 Amendments to the Computer Misuse Act (1990)

There have been a number of unsuccessful attempts to amend the Computer Misuse Act of 1990, which was finally successfully revised in 2006 by the Police and Justice Act (PJA). These are summarised in table 1 below and are discussed within the section that follows.

1990	**Computer Misuse Act (1990)** criminalizes 1. Unauthorised access to computer material 2. Unauthorised access with the intent to commit or facilitate the commission of further offences 3. Unauthorised modification of computer material
2002	APIG propose a new offence of “impairing the function” of a computer in order to legislate for DoS attacks. The private members bill received its second reading on 20th June 2002 but it proceeded no further.
2004/2005	APIG propose the creation of offences in connection with denial of service further provision for proceedings and penalties offence under section 1 of the CMA (1990)
2006	**The Police and Justice Act (2006)** amends the CMA (1990) in order to include DDoS attacks, to criminalize reckless behaviour, and the making and dissemination of hacking tools. Penalties under all sections of the CMA are increased.

Table 3.1 Development of UK Computer Misuse Legislation

On the 1st May 2002 a bill was introduced to the House of Lords for an amended CMA. A new offence of “impairing the function” of a computer was to be included in order to legislate for DoS attacks. The private members bill received its second reading on 20th June 2002 but it proceeded no further. The proposal referred to “computerised systems” rather than to “computers” but both terms were not clearly defined; changing terminology in this way without the provision of definitions leads to uncertainty about what acts should be included, thus often requiring further changes to made, or for judges to decide in court how the terminology should be interpreted or applied (Great Britain, Computer Misuse Act 1990 (Amendment) Bill 2002). As judges may not have expertise with technical jargon, this may not be wholly appropriate.

In 2004, another private members bill put forward by the All Party Parliamentary Internet Group (APIG) recommended that amendments be made. This proposal again resisted attempts to define terminology, so that courts could be left with the ability to apply the act according to contemporary usage of terms, stating that:

> We recommend that the government resist calls for words such as ‘computer’ to be defined on the face of the Computer Misuse Act and continue with the scheme whereby they will be understood by the courts to have the appropriate contemporary meaning.
>
> (APIG, 2004: 4)

It was felt that this would mean that the new legislation, when enacted, would remain applicable for a longer period of time, even if there were significant further technological advances, which would otherwise make the terminology obsolete.

It was suggested that Denial of Service (DoS) attacks must be fully covered by the act and also suggested was a shift in focus towards networks of computers, rather than individual machines in order to reflect the development of the technology.

A bill was printed on the 5th April 2005 which states its aim as being to:

> ..amend the Computer Misuse Act (1990) to create offences in connection with denial of service and to make further provision about proceedings and penalties for an offence under section 1 of that Act, and for connected purposes.
>
> (APIG, 2005: 1)

The proposed amendments finally came as part of the Police and Justice Act (PJA) 2006. The primary focus of the PJA 2006 was to make reforms to policing and to criminal justice, meaning that discussion around the control of cyber-crime was peripheral to the primary concern when the bill was debated and considered. Amendments were made to section 1 in the form of a number of minor additions. Section 2 was not amended, but the tariff was increased on indictment. Section 3 was completely replaced (Great Britain, the Police and Justice Act 2006).

The PJA (2006) made the unauthorised access offence in section 1 applicable also to enabling another to secure access, therefore widening the scope of the section. A section 1 access offence also became triable either way, rather than being only a summary offence, therefore making it extraditable. The perceived seriousness of the offence, and also the tariff were increased. A Summary offence under section 1 can currently lead to twelve months in prison (six months in Scotland) and a maximum fine of £5,000. An indictment under section 1 may lead to a two-year prison sentence plus fine (Great Britain, the Police and Justice Act 2006).

Section 3 of the legislation has seen the most dramatic changes, both in content and in tariff. The section was originally focused on the offence of modification of computer material. This wording has now been changed to "...unauthorised acts with the intent to impair, or recklessness as to impairing the operation of a computer". Section 3 is now worded in such a way that it is sufficient to cover Denial of Service (DoS) attacks which it had proved difficult to prosecute under the original act (CMA 1990) due to the fact that a DoS attack can make use of authorised rather than unauthorised functionality within a system. Erasure or modification is no longer necessary to secure a conviction under section 3, as long as there is intent or recklessness with regard to the likelihood of impairing functionality. The maximum tariff for a section 3 offence has been doubled from five to ten years imprisonment. The new wording differentiates this type of attack from criminal damage. The focus has moved from attacks against content to attacks, wilful or reckless, against network functionality (ibid).

Section 37 of the PJA 2006 adds a new offence of "…making, supplying or obtaining articles for use in computer misuse offences." The All Party Internet Group (APIG, 2004) had advised that this should not be legislated on due to the fact that researchers and Ethical Hackers will often need to make such Hacking tools in the course of their normal work, leaving them open to prosecution; the law makes no distinction between acts which are benign, and those that are malicious. This leaves the courts to decide whether the defendant believed that the tools they create, obtain or supply are likely to be used in the commission of any offence (Great Britain, the Police and Justice Act 2006) .

It has been suggested that the new tariffs and the making of a section 1 offence triable either way are excessive (Fafinski, 2009). In addition section 3 seems particularly excessive in cases where the cause was “recklessness” rather than being “intent” thus significantly changing the Mens Rea requirement for an indictment, APIG (2005) had originally suggested that this could more reasonably be divided into two separate categories of offence which would allow for differentiated levels of penalty to reflect the level of harmful intent.

The amendments have had some success; there has certainly been an increase in prosecutions and penalties. It would appear however that there are still a number of difficulties with terminology and with application which means that the legislation may still require further review, many respondents to this study indicated that they felt the law remains vague, is ambiguous and is out of date – their views and behaviour in relation to the legal framework will be examined further in Chapter Six. It has been argued that:

> A more effective response by the criminal justice system is in urgent need – because it would increase the number of convicted cybercriminals, and more important, because it would also have a preventive deterrent effect on the illegal parts of the hacking community
>
> (Bachmann, 2010: 653)

3.4 Alternative Modalities of Control: Code is Law

The law is not the only approach to dealing with the control of cybercrime. Larry Lessig (1999; 2001; 2004; 2007) describes a range of modalities of regulation which are utilised in cyberspace, and sees these as being related to those that are used in wider society. Core moral values in wider society are seen to be enforced through the Law, Architecture, Norms, and the Market. These modalities of control suggested by Lessig will be considered individually as they are the means by which professional standards may be reproduced in terms of an enforced 'ethic' for cyberspace.

Firstly, the law does have an important normative function as discussed in the previous section. It is enforced through ex-post sanctions such as fines or penalties. It is coercive in its logic in that it prescribes behaviour clearly, and is pedagogical in its approach in that it prescribes behaviour. This corresponds to the lowest level of moral reasoning according to Kohlberg's (1976) moral development taxonomy where individuals just follow laws or rules, and do not think through the ethical implications for themselves. In cyberspace this translates to previously existing law, such as those on copyrights and patents and also to specifically created laws, such as the Computer Misuse Act (CMA) 1990.

Secondly we have architecture, in wider society this will generally refer to physicalities such as buildings, structures, locked doors etc. As such it provides a form of control that is immediate rather than being ex-post and is self-enforcing. In cyberspace this architecture is the software, code, programmes and protocols which make up the environment. The self-enforcing architectural restrictions may take the form of username and password controls, cookies, filtering or SPAM. These can remove the autonomy, and therefore the liberty of the individual user, but only if the user does not have the technological knowledge to circumvent these. There are two main implications of this. Firstly it allows our behaviour to be regulated externally, in particular allowing for restrictive governmental or organisational control, ranging from for example the Chinese Government having full and unrestricted access to the machines of all users, to employers blocking employees from accessing social networking sites, and parents controlling the access of their children. The second implication of this is that this architecture may be circumvented, but only by those with specialist knowledge, altering the hierarchies of power within cyberspace so that knowledge and skill come to be expressions of power (Jordan, 1999). This allows some people not to follow the law, or to be able to construct and reconstruct for themselves the environment within which they operate. Lessig famously states that ‘code is law’ (2004, 2007) as he saw the use of computer code as being able to construct an architecture that would control online behaviour, and therefore we can see the power inherent in being able to write law for oneself, especially when it does not necessarily have to apply to others. The Hacker may be seen as circumventing the architecture, while the role of the Ethical Hacker is to utilise or to design this architecture in order to control the behaviour of others.

The third modality of regulation according to Lessig (1999; 2001; 2004; 2007) is the market. In wider society the market is able to regulate society through price, which is fixed through the market forces of supply and demand. This also is immediate rather than ex-post. In cyberspace we can see the impact of the market in advertising, types and availability of web services and pricing of services. In cyberspace the market can operate quite differently to how it does offline as it is subject to a different set of constraints. It is possible, for example, to advertise more widely or to sell products not available offline to ‘niche’ customers worldwide who may not all travel to a particular location, which may have meant that certain businesses could only operate online without going bust. For Ethical hackers the market that has an impact upon their behaviour is the market which buys their skills and services. As discussed in the previous chapter, many choose to switch from illegal to legal forms of hacking because the industry which has developed around hacking places a commercial value upon their skills and therefore allows them to earn a living by using their skills legitimately. Having well paid jobs and good career opportunities for those with hacking skills may provide an alternative route for those with hacking skills and prevent them from becoming involved in criminality.

The fourth and final modality is to be found within social and cultural or subcultural norms, which can be perceived as being an expression of the community and of its values. Norms refer to what is expected as normal behaviour. Lessig (2004, 2007) would locate ethics here, and has been subject to much criticism for this (Spinello, 2011) Where cultural norms are variable, culturally relative, and continually evolving, it is suggested that ethics should be related to 'meta-norms' (also known as 'natural laws') rather than norms, as meta-norms are universal, lasting, durable, transcend time and space, and are linked to human goods, rather than being culturally defined. Spinello (2011) makes the case that a more meta-normative than cultural stance is needed. It is argued that certain norms are universal and transcendental and that the focus should be upon these, rather than culturally bound systems of morality.

Foot (1979) lists a set of meta-norms which may be applied here. He describes the needs for affection, co-operation, and a place in society or within social groups, and help when in need as 'goods' which are desired by all humans. These 'goods' are emphasised in relation to a list of 'evils' to be avoided which include – feeling isolated, feeling despised and embattled, and being without courage or without hope. Foot suggests that these are universal human needs so would provide a useful standard rather than groups following separate sets of norms which are bound in cultural expectations. Social norms are expressed through community and can often take the form of labelling or stigmatisation when in their normative function.

In cyberspace this operates through the formation and reinforcement of social ‘netiquette’ and the associated labelling of for example ‘flaming’, ‘spamming’, or ‘trolling’ which are almost universally unacceptable forms of online behaviour.

Lessig’s (2007) constraints on cyberspace can be criticised as they are rather determinist. They show a range of possible behaviours afforded to the individual, the afforded being restricted by the four modalities of regulation, the strongest of which Lessig (2004, 2007) believes to be code, leading Lessig to consistently claim throughout his work that ‘Code is Law’. As we have seen however, all of these, even code may be circumvented. It would appear that none of these modalities of control can be completely effective in ensuring that the Ethical Hacker remains on the right side of the law. In the next section we will consider some of the internalised morals and ethics which may have more of an impact than the external controls that have been described here.

3.5 Ethics and Morality

Any examination of the nature of ethics and morality must commence by considering the difference between these two overlapping, and frequently confused concepts. It has become apparent in the interviews which have been conducted during the research that the respondents either perceive these to be mutually interdependent or are otherwise unable to differentiate between the two, and in some cases will use the terms interchangeably. Stamatellos (2007) is also indicative of this confusion in his description of ethics as being a system of morality.

Tavani (2011) defines both terms for us distinctly, and it is here that we can begin to examine the nature and meanings associated with the terms, as well as how they relate to one another. Both terms appear to be commonly used to describe a ‘system’ which in some way provides a set of rules for governing human behaviour, and in particular, for governing social behaviour. In effect, the systems can guide human behaviour by establishing a framework of customs, habits, behaviours, social norms, expectations and values by which we are able to judge our own behaviour, as well as that of others. At first glance it would appear that the main difference between these apparently similar concepts is the root of the words and the way in which they have developed. ‘Ethics’ comes from the Greek ‘ethos’, connoting the environment, or the mood, where morality can be understood in relation to its Latin root ‘mores’ which pertains more to social values. As we will see within the following section morality describes a very fixed set of behavioural rules; ethics can either be normative and therefore are able to function in the same way as a moral system, or can be flexible, and therefore dependent upon the situation and the stakeholders.

Morality is further described as being a purposive system, the aim of which is to prevent harm or detriment to self, society or other individuals (Gert, 2004a; 2004b; 2005).

> Morality is an informal system applying to all rational persons, governing behaviour that affects others, and includes what are commonly known as moral rules, ideals and virtues, and has the lessening of evil or harm as its goal.
>
> (Gert, 2004b: 98)

This approach to morality as a system of impeding evil further raises the question of whether it should promote flourishing or ‘good’ , and if so, then what is meant by ‘good’? If evil is to be understood as the impedance of good, then we must unravel these terms in relation to one another. According to Reynolds (2013) “…morality refers to social conventions about right and wrong, they become the basis for an established consensus" (Reynolds, 2013: 3).

Within the ethical approach of 'natural law', moral norms can be understood as being absolute, and of themselves, rather than being social constructs. Aquinas asserts that our behaviour should follow the adage that good should be done and evil avoided (Davies, 1993). This raises the further question of whose definitions of good and evil should we follow? (Spinello, 2011). In fact as we have already discussed within this chapter, these are normative concepts and therefore are culturally bound, and must be transcended in order to allow any kind of universal system that can be followed.

Finnis (1983) described seven 'goods' which were perceived to be of equal worth or merit. These were 'life and health', 'knowledge of the truth', 'play and work', 'aesthetics', 'sociability', 'religion' and 'practical awareness'. An Aristotelian approach would suggest that these all lead to human happiness, and are therefore essentially the same in their nature (Hope, 2010).These approaches can be criticised for not defining these goods in relation to 'evil' (Foot, 1979). Rather than being specific about the nature of evil, it is seen only as the impedance of good.

Beauchamp and Childress' (1984) 'principlism' highlights four conflicting goods. The first of these is 'autonomy', or the ability to be independent in action and thought. It can be considered to be closely related to the notions of individual liberty or freedom. The second of these is 'non-maleficence', commonly understood in relation to the medical approach inherent within the Hippocratic Oath; it insists of an approach of doing no harm. It does not necessarily have any expectation of doing good, other than that it does not allow for harm, or negative or 'evil' impacts. The third principle is 'beneficence', which involves the active promotion of positive 'goods'. It gives the imperative that we should be expected to make a positive difference to those around us. This principle instructs us to help those in need, particularly those in urgent or serious need. This, of course, relies upon our ability to perceive this need, or to have prior knowledge of said need, and also to have the capability and the resources to respond to it. The fourth principle within the system is 'Justice'. It refers to a natural or equal justice as defined by Rawls (1971) who suggested that the only true justice was one in which a person writing social rules was not aware of their own social characteristics and therefore would not favour any one group above another, based upon any of the normal stratifying characteristics. This notion of justice is therefore related closely to socialism and the advocacy of equality.

Beauchamp and Childress (1984) go on to consider the implications when any of these principles are found to be in conflict with one another. They suggest that our conduct should then be governed by a questioning of whether there is any possibility of honouring more than one, and ideally, all of the principles. It is not always possible to differentiate between the values of the different 'goods' (Finnis, 1983). Beauchamp and Childress (1984) would advocate that this is necessary, and must be judged upon which approach is most likely to deliver a substantial outcome. This cannot be prescriptive as it will vary from one situation to another, so must be judged on a case by case basis.

Ross (1930) furnishes us with yet another list, some of which overlaps with the previous lists of principles or 'goods'. These are 'fidelity', 'reparation', 'justice', 'beneficence', 'self-improvement', 'gratitude', and 'non-injury'. Again, we could criticise by stating that there is no ordering, and that these principles lack universality. As with Beauchamp and Childress (1984), this system could be defended by saying that ordering would depend heavily upon the situation, and also upon the individuals involved, so that a generic or universal system of ordering is not possible.

Tavani (2011) describes ‘morality’ for us as being a system of rules or principles which include individual directives at a micro level, and social policies at a more macro, or societal level. It is here that we can differentiate clearly between moral systems of rules, and guiding principles, which seem to have a fairly clear-cut idea of what is, or is not acceptable; it may therefore be considered as a fairly ‘closed’ system; its logic being Boolean, digital, absolute. Ethics, it will become clear, is a much more problematic area, being very ‘fuzzy’ in the nature of its logic, and therefore struggling, in the main, to define the structure of its own system; where moral systems may struggle with ranking of ‘goods’, ethical systems struggle to identify the very nature of good and bad. They variously consider virtue and intent, actions, and consequences, and lead us to the conclusion that there are not, and cannot be, any absolutes in what is, or is not, acceptable human behaviour. Where morality struggles with ranking and universality, ethics says that sometimes doing harm can be ‘good’; if it is done with good intentions, or if it leads to positive outcomes.

Stamatellos (2007) again fails to differentiate clearly. He sees ethics as being related to decisions we make regarding freedom, privacy, equality, duty, obligation, choice and any related judgements, rights or claims. We can clarify this position by considering how the relationship between ethics and morality is perceived, this elucidates for us why it is that they are defined in such similar terms. Stamatellos (2011) describes ethics as being principles which guide our morality, and therefore they are very closely interlinked. As an open system, or range of systems, the nature of meta-ethics and normative ethics therefore require further attention.

Levy (1984) describes his understanding of Hacker ethics and beliefs. The first principle is that computers, or any other means by which we can educate ourselves, should be free and unrestricted. Hackers should learn pragmatically, by Hacking, so must have the technology available to them; we should all, according to the hacker ethic (Levy, 1984; Himanen, 2001) have the right to have access to knowledge. Power is increasingly held in technology and the ability to manipulate it and so the decentralization of power requires the decentralization of technology. Hackers will be judged by their Hacking skills and knowledge rather than by offline prejudices based on socially differentiating characteristics such as age, class, or gender. It is also a principle within Levy's (1984) 'Hacker Ethic' that art and beauty can be created on a computer. Computing and technology is seen as a revolutionary resource with the power to create a better society (Levy, 1984; Hollinger, 1991). The Hacker Ethic (Levy, 1984) is thought to have became a cultural norm, rather than being something which was overtly commented on or discussed within the community (Wark, 2004).

There are a range of normative and philosophical approaches to making ethical decisions. Within each of these approaches there are three basic stages in decision making:

1. Identify a moral problem or controversial issue
2. Clarify/define the related concepts and ideas and then collate and examine the facts
3. Apply a range of moral theories and principles in order to reach a conclusion

(Brey, 2004)

This formulation from Brey (2004) is suggestive of the usefulness of a Bounded Rational Model in understanding the decisions that are made in relation to moral behaviour. Stage 2 is suggestive of a reasoning process, and stage 3 identifies the application of theories and principles; this application is clearly bounded by knowledge of these theories and principles, and also by perceptions relating to their importance.

This process is often not applied methodically, but rather it is dependent upon community norms and socialisation; a person may also have their own preferred approach based upon previous experience and frame of reference. It is essential for the Ethical Hacker to remove himself from personal philosophical set of beliefs and to locate their behaviour within a set of professional standards rather than philosophical ethics so that behaviour is more consistent within the professional field.

3.5.1 Virtue/ Character Ethics

We can consider ethical action as being a personal virtue, or character based issue. This idea is often linked to the ethical approach of Aristotle (Hope, 2010), and looks at why we act the way we do rather than the actual actions we perform or the consequences of these actions. Aristotle believed that all of the ’goods’ that we seek relate to human happiness. In this approach it is possible to excuse bad actions or bad outcomes, as long as the individual acting had good intentions in carry out these actions. There is the assumption that a good or virtuous character can be developed through a developed or advanced moral Education. Kohlberg (1976) tells us that those among us who opt to follow rules do not all do so for the same reasons, but that the reasoning is variable based upon our level of moral understanding; this necessitates the development of this moral reasoning rather than simply teaching people to obey rules, or expecting them to abide by contracts or standards.

Kohlberg's (1976) model is split into three stages, with two levels within each stage. Stage one is called ‘Pre-conventional, and at the most basic level, we act, or obey rules, in order to avoid punishment; we are driven by the need to avoid negative sanctions

In the more advanced level of stage one this is replaced by behaviour in which we follow rules in order to benefit the self. This could include staying on the right side of the law in order to remain employable.

In stage two of his moral development framework, which Kohlberg (1976) calls the ‘Conventional’ stage, we act as we do in order to gain group approval, so at this level of development we are thought to be more responsive to social norms than at stage one. In its more advanced form, stage two behaviour sees us as having a belief in the social order and a need to re-affirm and support that order by obeying rules or social norms.

At stage three, the ‘Post-conventional’ stage, this comes to be a desire for a more formalised system as the social contract is seen as being mutually beneficial to all of society. The upper level within the third stage perceives the social actor as being driven by a personal commitment to social justice and egalitarian principles. Kohlberg (1976) argues that obeisance is not ethical or moral in and of itself, but, rather, it is driven by how far we have advanced through this taxonomy of moral reasoning. Morality is therefore understood to be relative to how morally developed our characters are rather than how we act. By being more morally developed we can be considered to be more ethical, ethics are not simply bound to what we do, but also relate to why we follow rules.

McQuade (2006) concurs with this view. He suggests that education is necessary for making ethical hackers follow the professional standards of their industry. He states that:

> Through education and training people can better understand the rationale behind these rules, internalise potential harms and sanctions for non-compliance, and choose to abide by organisational and societal standards of behaviour on the basis of logic and reason for the common good of everyone
>
> (McQuade, 2006:144)

This would suggest that in order for normative approaches to be adhered to, they must be underpinned by a meta-ethical understanding. This is idea would be supported by Kohlberg (1976) who suggests that advanced moral reasoning advocates rule following, but only where the rationale behind these rules is understood, which will be considered further in the following section.

Virtue/character based ethical approaches may be criticised as they do not consider the impact of a lack of community homogeneity of variance in relation to morality, professional standards or other rules of conduct which guide our behaviour (Tavani, 2011). Ethical Hacking lacks this homogeneity of variance, and as we will see in chapter 6, this is because the respondents employ different ethical stances in their decision making approaches.

3.5.2 Deontological Ethics

Secondly we turn to deontological approaches. These focus on our duties under contract or under moral obligations. The focus is on our actions and how these relate to the formal and social rules which we are expected to follow and which we expect that others will follow. Kant (1959) argued that all actions are intrinsically either right or wrong, and therefore we should apply the principle of Universalism. Kant (ibid.) saw the human condition as being rational and reasoning (Tavani, 2011; Prenzler, 2009) he would have criticised intent based approaches such as that of Aristotle as we do more than seek out happiness, and in fact sometimes, the ‘right’ thing to do will make us unhappy (Tavani, 2011). Rather than just being guided by whether a particular action will make an individual happy, Kant would suggest that all action should be driven by whether we would want all other actions in the future to be the same; therefore we should only steal for example if we think that this is acceptable for everyone, at any time to do the same. Kant (1959) is suggesting that we should behave as though our actions were setting a new command/rule, or imperative for further action. An imperative might be hypothetical/theoretical (in the case of A, do B), or may be categorical (do A, OR, Do not do A). Kant only advocates one categorical imperative and it links to the further promotion of freedom and rationality by suggesting that we should act towards others as we would want to be treated. This approach advocates objectivism and need for universalism, whereby all rules would be understood in the same way, and equally adhered to by all members of society (Ess, 2006) due to the pluralism in rule or norm setting and following which suggests that in fact there are multiple rules, and multiple interpretations of them.

Ethical formalism does not completely disregard virtue or character based ethical systems, but rather it builds upon them. In order for an action to be good, it must not only be good, but must be for good intentions, and also must be freely chosen. We are not therefore ‘good’ because we follow rules, or fear sanctions. We are good if we follow good rules because of good intentions and good moral reasoning (See also Kohlberg, 1976). We can therefore judge people by a combination of their actions and intentions, but not by either alone. A difference between action and intent based ethical reasoning is that people come to be seen as ends in themselves rather than means by which some other end can be achieved. Ethical formalism allows for the creation of a set of standards to be followed universally and is therefore the main form of reasoning to be utilised in the creation of the criminal law, however its absolutism is tempered by other reasoning and mitigation when presented in courts of law (Prenzler, 2009). Kant (1959) argues that the self must be deleted from reasoning, in common with Rawls (1971) formulation of the nature of ideal justice, because the self cannot be excepted from the absolutism or universality of any established rules or duties.

Tavani (2011) differentiates between deontology that is based upon rules, and that based upon actions. Both of these deontological approaches advocate that ethical behaviour is related to notions of duty, the distinction being whether the focus of ethical choices should be personal behavioural choices (act deontology) or how we would like others to act in the future (rule deontology).

3.5.3. Teleological (Consequential) Ethics

Utilitarianism, in common with deontology, can either focus upon either rules or upon acts. It is focused upon the consequences or outcomes of our behaviour rather than the motivations and intentions which drive our behaviours, or the actions in themselves. It is described as being a teleological theory in that the ends are perceived to justify the means, so that the outcome of an action justifies the process. In common with virtue or character ethics, utility stresses happiness, but seeks to measure this at a more societal and consequential level. An ethical decision carried out from within this approach would seek to balance the amount of pain caused by an act or rule in such a way that the pleasure the act causes outweighs the amount of pain caused. The utilitarian approach is known for seeking 'the greatest good for the greatest number' – the utility sought is not then individual or egoistic utility, but rather it is utility at a societal level. The approach is to be found within the work of Jeremy Bentham (1781), J.S. Mill (1806-1873) and G. Moore (1903). A simple cost/benefit analysis is carried out which may produce the best outcome for the whole social group, however it is ignorant towards social justice for the individual, for the few, or for the self. As we shall see in chapter 6, Ethical Hackers are concerned about others, but they are also concerned with the outcomes for themselves.

3.6 Meta-ethical Approaches to Underground Hacking

Approach	Focus	Examples from the Underground
Virtue/Character	Intent	True Hackers'
Deontological	Action	FOSS
Utilitarian	Outcome	Hacktivism'

Table 3.2 Meta-ethical Approaches to Underground Hacking

The three meta-ethical approaches outlined in the previous section can be linked to the typologies that were discussed in chapter 2. Table 2 above gives some examples to illustrate the usefulness of meta-ethical approaches in understanding hacking behaviour. True Hackers as described by Levy (1984) can be understood as virtue/ character Hackers. The Hacker ethic that was described by Levy (1984) and Himanen (2001) makes it clear that Hackers should be driven by positive intentions to do good for society, to share information, and to treat each other without regard to the inequalities that are inherent in wider society. FOSS hackers can be understood as deontological, in that they are focused on actions, and that they follow rules set for them (they do not break the law), but also behave in a way to set standards for others to follow in line with Kant's (1959) categorical imperative. The behaviour of Hacktivists (Taylor, 2000) is teleological; they are happy to break the law if they perceive this to be for a just cause. Please note that the above are examples only, and are not exhaustive lists from the typologies, but merely serve to illustrate the usefulness of the model, which will be further discussed in chapter 6 in relation to Ethical Hackers.

3.7 Summary and Conclusions

Hackers were influential in the development of computing and networks. The technology created was also in turn influential in the development of hacking and the community which surrounds it. From this arose a new set of opportunities for social engagement and also for crime and its control. Cyber-crime has created the need for developments in the law in order to control it, and to placate the public who were becoming concerned by developments in technology, which seemed to be creating whole new set of crimes and criminals. These new laws have further criminalized a set of activities, some of which were malicious and dangerous, but many of which were benign.

In addition to the legal framework, other forms of control have been found to be important in the regulation of cyberspace. These include the use of computer code, and normative and meta-ethical approaches.

In the following chapter we will examine the methodological procedures and choices that are used to realise the analysis of the bounded decisions of Ethical Hackers with regard to criminality, criminal events, and desistance form offending.

Chapter 4: Understanding Ethical Hacking Through Realist Research

4.1 Introduction

This Chapter aims to outline the methodological issues and the many choices that relate to the design and to the conduct of the research. The development of technology and of Hacking as an activity has created the need for the 'Ethical Hacker' who is understood as being an individual who utilises Hacking skills and knowledge, but does this within legitimate authorised practice.

As identified in Chapter 2 there is a gap in the current literature in relation to the newly emergent field of 'Ethical Hacking.' The literature which is available relates to Hacking rather than to Ethical Hacking, and tends to be focused upon typologies, and upon criminality. This study aims to utilise a Critical Realist methodology, with the use of semi-structured interviews in order to begin to address this gap in order to understand the 'Ethical Hacker' in terms of the motivations, the decisions and the social structures that inform the practice of 'Ethical Hacking'.

This is achieved by looking at the structures and practices which inform the reasoning of the Ethical Hacker in the decisions that are made about how to practice.

The main method that has been employed is the semi-structured interview which was selected in order to collect the personal stories of the respondents for analysis. Methods of data collection and analysis will be discussed, followed by consideration of issues relating to the validity and reliability of the data produced.

There is a wide-ranging literature available, which describes the qualitative tradition in social research, and how to design, carry out, analyse, and present the data generated (Hammersley and Atkinson, 2007; Bryman 2008). This literature will be discussed within this chapter in order to illustrate the rationale behind the methodological choices which have been made.

The study is distinct and creates an original contribution to knowledge by offering an exploration of a newly emergent and still developing social group. An examination of this group may add a new category to those already established and accepted typologies extant within the available literature. The research provides potential to develop an understanding of the life course, motivations, relationships and practices of the Ethical Hacker and the social world in which he operates.

4.2 Theoretical approach to the research design

This study is underpinned by Critical Realism: a multifaceted construction of methodological and theoretical thinking that has emerged since the mid 1970s. Critical Realism views reality as having an existence that is completely independent of social constructions (Archer, 1998; Bhaskar, 1975). A key figure within the Critical Realist movement is Roy Bhaskar, who started to develop his ideas through a close examination of the philosophy of natural science. As a theoretical concept, the idea of 'realism' suggests a view of the world that recognises the materiality of social facts whereas the 'critical' part of the approach problematises the empiricism within natural science (Danermark et al., 2002; Maxwell 2012).

Bhaskar (1975) critiqued ‘empiricism’ as reducing reality (and therefore research), to only that which is observable. Critical Realism seeks to analyse that which cannot be seen or instantly grasped. This then constitutes a holistic approach that is able to understand reality as having an existence beyond the subjectivity (relativism) of the individual or that of social constructivism (Sayer, 2002).

From a Critical Realist perspective there are three levels to reality, the ‘Real’ (generative mechanisms), the ‘Actual’ (everything that is observable, whether observed or not), and the ‘Empirical’ (that which is observed or measured. The approach “claims to be able to reconcile ontological realism, epistemological relativism and judgemental rationality” (Archer et al, 1998; xi) This is the case because reality is “stratified, differentiated structured and changing” (Danermark et al, 2002;10), and our knowledge of reality is fallible, but we can distinguish between theories (Danermark, 2002) Being is therefore real, knowledge is relative, knowledge, over time, can improve and can get nearer to reality as we distinguish between theories.

One of the central tenets of Critical Realism’s research design is its flexibility; it having the capacity to allow reflection upon what is really happening during the research process and to respond reflexively. There can be many unanticipated challenges and barriers that the researcher is not aware of at the outset of conducting qualitative research; the actual research environment and respondents therefore need help to shape the research process. Even where the researcher has preset ideas about the design of the research or the potential findings, qualitative research demands that the researcher is able to be responsive to external influences and factors, particularly those from the subjects of study, allowing these to shape their perspectives, in order to negate the impacts of these preconceptions for the outcomes of the research.

Many sociologists perceive there to be a natural bifurcation between naturalism and constructivism. Naturalists or realists tend to believe in the objectivity of social reality. Constructivists on the other hand do not believe in the objective reality of social existence but rather believe that society is constantly created and recreated through the interpretation of social action (Maxwell; Danermark et al 2002). "The division between the general and the unique has marked the discussion of qualitative and quantitative method" (Danermark et al, 2002: 75)

It is questioned by Critical Realists whether it is necessary to see the two approaches as being naturally opposed; "the traditional dichotomy between quantitative and qualitative methods is unproductive" (Danermark et al, 2002: 175). It may be more useful to combine these micro and macro approaches to come to some kind of common-sense meso approach (Chamberlain, 2013). The proposed research begins from the ontological perspective that social reality has some level of objectivity but also that this objectivity is partially constructed through the interactions and interpretations of individuals. This has interesting implications for both the epistemology within the paradigm being followed or created, and for the choice of methodological framework, methods of research and analysis.

According to the naturalist approach, the central concerns are 'what' questions e.g. what has happened? What does it mean? For the constructivist the central questions of concern to the researcher will be 'how' questions, for example, *how* social activities are carried out (Gubrium and Holstein, 1997). The Critical Realist moves beyond these questions, rejecting them as only uncovering the empirical, and not having the ability to access the actual or the real (Bhaskar, 1975; Danermark et al, 2002). For the critical realist, the key question is not what happened, or how did it happen, but rather the underlying generative mechanisms are sought (Bhaskar, 1975; Danermark et al, 2002). Because “models based exclusively on the empirical level do not have the capacity to take into account the generative structures” (Danermark, et al 2002: 172)

Denzin and Lincoln (2011) suggest that it may be useful to address social research as a continuum, within which the researcher is able to take what is useful from within the existing paradigmatic approaches. “Although some researchers do adopt an extreme positivist or extreme constructivist stance…reality may lie somewhere in the middle of these two poles in our continuum” (Chamberlain, 2013: 108). This has led to the choice of Critical Realism as the underpinning philosophical approach to the research conducted here.

Critical realism combines:

> A realist ontology (the belief that there is a real world that exists independently of our beliefs and constructions) with a constructivist epistemology (the belief that our knowledge of this world is inevitably our own construction, created from a specific vantage point, and that there is no possibility of our achieving a purely “objective” account that is independent of all particular perspectives). All knowledge is thus “theory-laden,” but this does not contradict the existence of a real world to which this knowledge refers.
>
> (Maxwell, 2012: vii)

It is necessary to take an intensive approach to data when exploring new ground (Danermark et al, 2002) as there are often no theories or models which can offer a framework, and the job is therefore to create these, however this does not negate the fact that “meaning and culture are real” and “causation is real” (Maxwell, 2012: 1).

The initial aim is to uncover the realities of a range of respondents, which also influences the choice of methodological approach as “…when researchers conduct qualitative research, they are embracing the idea of multiple realities” (Cresswell, 2013: 20). The reality of Ethical Hacking for each of the respondents is a different reality. For Critical Realism though, this level of analysis is not enough, as it reveals only the empirical level. It is therefore necessary for the researcher to interpret the data in order to uncover the underlying generative mechanisms which explain the occurrence of the empirical.

Epistemological issues are those which refer to the very nature of knowledge and the standard question posed in relation to this is what level of level or type of evidence will be acceptable to the researcher in proving that the outcomes of the study are valid. In this case, the level of proof will be interpretive.

While this approach makes generalisation, replication or falsifiability difficult, it does ensure the production of a set of data which will be rich, meaningful, and informative about motivations, about culture and about behavioural norms. The aim is not generalisation or replicability, the aim is to access the level of the 'real' in order to explain the mechanisms which underlie the choices that are made by Ethical Hackers.

Danermark et al (2002) explain why CR is a useful approach:

> Just as the physical world is extremely complex but can be seized in some fundamental traits, the same goes for the social world. 'That social behaviour is complex cannot be denied, but the principles governing this behaviour need not be complex', says The Social Science Encyclopaedia (Doreian, 1985:504). An example of this is rational choice theory, the basic idea of which is that 'when faced with several courses of action, people usually do what they believe is likely to have the best outcome' (Elster, 1989:22).
>
> (Danermark *et al.,* 2002: 172)

	Empirical Quantitative Enquiry	Naturalistic Qualitative Enquiry	Critical Realism
Analytical Logic	Deductive	Inductive	Retroductive/ Abductive
Ontological Perspective	One reality	Multiple constructed realities	Three layers to reality – empirical, actual and real The 'Real' is intransitive
Epistemological Perspective	objectively knowable	Interpreted subjectively	Knowledge is transitive

Table 4.3 Analytic Logic, Ontology and Epistemology in Critical Realist Research

Table 3 above shows the differences in the ontological, epistemological and analytical approaches taken within positivistic, naturalistic and Critical Realist enquiry.

As has been discussed (see chapter 2) Ethical Hacking is a relatively new social phenomenon, and therefore it has been appropriate to undertake its study from a Critical Realist perspective. The inherent flexibility, reflexivity and philosophical approach to knowledge have allowed this research to uncover generative mechanisms for behaviour, social organisation and motivations that were at the outset unknown. The choice was made to use traditional qualitative methods because "We conduct qualitative research because a problem or issue needs to be explored" (Cresswell, 2013: 47). In Critical Realist research, qualitative methods are utilised within intensive research designs as will be outlined in the following section.

4.3 Intensive Research Design

Although the methods employed are identifiable with the gathering of traditional qualitative data, the term 'intensive' is employed here rather than the term 'qualitative' in order to differentiate the approach taken from that of the traditional qualitative approach, whose ontological perspective, and empirical approach are here rejected as being only able to uncover constructions rather than reality (Harre, 1979; Sayer, 1992; Danermark et al, 2002), and being confined to the level of empirical knowledge (Bhasker, 1978), without having access to the 'real', the generative mechanisms which are sought through critical realist research (Danermark, et al, 2002).Critical Realism was adopted as "…realism helps to resolve some of the serious philosophical, theoretical and methodological problems that qualitative researchers face" (Maxwell, 2012: ix). It has allowed "…a commitment to the existence of a real though not an objectively knowable world" (Maxwell, 2012: 10).

The research undertaken is an intensive study, the primary goal of which is to understand the activity that has recently come to be termed as 'Ethical Hacking', its development as an individual and social phenomenon, and the social context within which it takes place. The reason for this choice is that qualitative, and therefore intensive, research design can allow us to explore complexity, to pass on stories, to understand contexts, and to develop theories (Cresswell, 2013) as well as to identify mechanisms (Danermark, *et al.*, 2002).

The research will be framed within the interpretive epistemological approach, and acknowledges that the data gathered cannot exist independently of the researcher (ibid.), but rather it is influenced by the numerous choices made within the design. Social reality is perceived to be in a constant state of flux due to the continual creation and recreation of it through our interactions and communications with one another, this necessitates an acceptance that the interaction between the researcher and subject may influence the outcome. Whilst the knowledge that we have may be transitive, this in no way negates the intransitive nature of the reality which is described (Bhaskar, 1975).

The researcher will also have preconceived ideas, which may impact upon the research. In this case the researcher had prior experience of teaching in Criminology with regard to the impacts of information communication technology for crime prevention. This meant that much of the prior knowledge was from the perspective of crime control of criminal hackers, and also that the knowledge was academic, rather than based in real world experience. The review of the literature revealed that much of the available literature added to the demonization and pathologising of the activity of hacking, by being focused upon those who had been prosecuted for criminal acts and how they could be controlled. The decision was made that the research should be appreciative in order to present the stories of ethical Hackers from their own viewpoint, as the narratives of those engaged in hacking have largely been ignored by academia (please see Chapters Two and Chapter Three for a full discussion).

Goffman excuses himself from the partisanship that exists in social research by stating that “...the imbalance is at least on the right side of the scale…” (1968: 8) What he means by this is that the researcher empathises with the person being researched and produces data that may be described as being appreciative. They are commonly known as ‘committed’ sociologists, and aim to take the side of the marginalized or previously unresearched, in order to give an appreciative account of their social life. This approach is common among ethnographers and qualitative researchers who feel that it is necessary to produce studies, which are not necessarily objective, in order to be able to represent the views of the marginalized in society whose views and opinions are not understood. This was essential for this study as the Ethical Hacker has not been previously examined, and an appreciative perspective would provide an account that is true to the reality of the respondent, and therefore a valid account of the empirical level of experience. Validity is further discussed in the following section. Critical Realism however rejects the naturalistic enquiry approach to reality as advocated by Lincoln and Guba, (1985; see also Guba and Lincoln, 1989). Naturalistic Enquiry advocates multiple constructed realities whereas for the Critical Realist the ‘Real’ is the intransitive object of research.

From a Critical Realist perspective this is only the first stage of the research, and only reveals the empirical level. The researcher must take this further by establishing demi-regularities (Lawson 1997) and transfactual conditions in order to gain an understanding of the generative mechanisms which create and explain the behaviour. Whilst the empirical level can be relied upon to reveal itself to some extent, the generative mechanisms cannot. Social systems are complex, and without ‘closing the system’ by controlling all variables these mechanisms “cannot always manifest themselves empirically” (Danermark et al, 2002: 163), mechanisms can be “reinforced, modified or suppressed” (Danermark et al, 2002: 163) in a complex system.

Because we cannot close the system by excluding all variables, and because the reality of a generative mechanism does not always mean that it is revealed at the empirical level, it is necessary to use abductive and retroductive reasoning in the analysis of data, rather than the inductive and deductive logics that are traditionally employed in the qualitative and quantitative research paradigms.

The methodological framework allowed for a detailed examination of the personal journeys made by Hackers when they chose to become contracted or salaried to provide security solutions to business, industry and law enforcement.

Although it was decided that an intensive approach was necessary as there were no previous models or theories that could provide a framework, and also because of the difficulties in accessing large samples, the field to be examined is no less ‘real’. Ethical hackers are real people, in real jobs, with real social networks and real histories. The use of an intensive design does not mean that the researcher can assume that there is no ‘realism’ in the experiences and the lives of those being studied. Although the small sample size may be criticised for lack of generalisability, generalisation should not be the aim of all research. It is necessary that some of the data produced in social research is rich in exploring detail so that studies may produce a range of types of information to create a fuller picture (Denzin, 1983).

4.4 Establishing Trustworthiness in Critical Realist Enquiry

Qualitative research has attempted to establish credibility by equivalence with measures of trustworthiness as applied in traditional positivistic research. Lincoln and Guba (1985) identify four measures of trustworthiness as employed in the natural sciences and suggest parallel criteria which are to be used in what they term 'naturalistic enquiry'. This is further developed in the following section in order to show how trustworthiness is established in Critical Realism.

In the natural sciences internal validity is used as a measure of 'truth value'. Internal validity can be understood to be the extent to which research represents the field which it is attempting to describe. Questions relating to the validity of research are generally understood to relate to whether we are measuring what we think we are measuring, whether a true representation of social reality is created (Marsh and Keating, 2006). It is usual to distinguish between…

> …internal and external validity, where internal validity refers to the ability to produce results that are not simply an artefact of the research design, and external validity is a measure of how far the findings relating to a particular sample can be generalized to apply to a broader population.
>
> (Elliot, 2005: 22)

In naturalistic enquiry the concept of internal validity is replaced by the concept of 'credibility' (Lincoln and Guba, 1985: 301), which can be established by prolonged engagement in the field, persistent observation, triangulation of both sources and methods, peer debriefing, negative case analysis, referential adequacy and member checks (Lincoln and Guba, 1985). For the Critical Realist neither approach is adequate for establishing truth; both being limited to the level of the empirical. As we have seen, the Critical Realist believes that 'the Real' is not revealed in the empirical (Bhaskar, 1975; Danermark et al 2002), hence the establishment of truth in the collection and verification of empirical data is criticised as an 'epistemic fallacy' in that the three levels of reality are reduced to the empirical, and the underlying generative mechanisms are not revealed.

The second measure of authenticity discussed by Lincoln and Guba (1985) is 'applicability'. For the natural sciences this is measured as external validity, and can be understood as the extent to which the findings of research are generalizable (and therefore applicable) to the wider population. Lincoln and Guba (1985) suggest that naturalistic enquiry within the qualitative tradition can replace this measure of applicability with what they term 'transferability' (1985: 316). It is suggested that a working hypothesis which is constantly re-evaluated in the midst of thick description will ensure that findings are transferable to other cases. For the Critical Realist the aim is to describe the 'transfactual conditions' (Danermark et al, 2002:78) which reveal the underlying generative mechanisms of social behaviour, and can be verified through 'demi-regularities' (Lawson, 1997). For the Critical Realist there is no pretence of generalizability (Sayer, 1992), instead, the suggestion is clear that the unusual, the unrepresentative "may reveal more about the general processes and structures than the general one" (Sayer, 1992: 249). Sayer (1992) suggests that even though individuals and the events that they are involved in may indeed be unique, that the generative mechanisms which define their behaviour may be understood through abstract concepts which are generalisable.

The third measure of authenticity defined by Lincoln and Guba (1985) is consistency. In the natural sciences this is associated with replicability. This is equivalated in naturalistic enquiry with 'dependability' (Lincoln and Guba, 1985: 316). Firstly, they suggest that dependability can be asserted through the presence of credibility, through overlapping methods, through ‘stepwise replication’ so that all researchers within a team conduct the research in the same way, (1985: 317) and through auditing the enquiry by examining closely the research processes and product. For the Critical Realist consistency can be measured through ‘corroboration’ (Sayer, 1992:246) “we must distinguish between testing to see how general the particular findings are in the wider population (replication) and testing to see that the results really do apply to those individuals actually studied (corroboration)” (Sayer, 1992: 246). The aim of replication is possible, but only within extensive rather than intensive research designs. In intensive research design replication is not the aim, and thus the Critical realist would assert that the starting point must be to consider that aims established by the research question (what is it that we want to know) and to decide upon the use of intensive, extensive, or mixed methods as appropriate (Danermark, 2002).

The final measure of authenticity as discussed by Lincoln and Guba (1985) is that of ‘neutrality’, which is measured in the natural sciences as ‘observer objectivity’. There is expected isomorphism between the data and reality. According to Danermark et al (2002:23) “Reality exists and is what it is, independently of our knowledge of it” which is in contrast to the aim of the isomorphism of the natural sciences. Lincoln and Guba (1985) reject observer objectivity as being impossible, due to interpretation by the researcher which can only be done through their own frame of reference, and through the lenses of culture, knowledge and experience. Rather than observer objectivity, the naturalistic enquirer seeks the ‘confirmability’ (Lincoln and Guba, 1985: 319) which considers the observed’s objectivity rather than that of the observer. The Critical Realist would reject both observer and observed objectivity, as both merely reveal the empirical, and cannot access the actual or the real, seeing knowledge and theories as transitive, and only the ‘Real’ as being intransitive. Reality then is the intransitive object, but it is not objectively knowable.

In Summary, naturalistic enquiry proposes four ‘parallel criteria’ (Lincoln and Guba, 1985; Guba and Lincoln, 1989) for assessing the truthfulness of social research findings. Credibility, transferability, dependability, and confirmability come to replace internal validity, external validity, replicability and observer objectivity in evaluating research findings. Guba and Lincoln (1989) later added ‘authenticity’ as a criterion for evaluation; this having no equivalent within the positivist paradigm, and being focused mainly upon the outcomes of research rather than its conduct. This measure too is rejected as being relativist, and failing to go beyond a consensus on empirical knowledge (Maxwell, 2012).

Critical Realism rejects both approaches as they fail to establish any truth beyond the empirical level, and therefore cannot access the generative mechanisms which explain behaviour (Bhaskar, 1975; Maxwell, 2012; Danermark at al, 2002). “This position essentially reduced ontology to epistemology” (Maxwell, 2012: 128) and therefore Critical Realists rather attempt to describe the transfactual conditions which underlie social behaviours; they believe that ‘demi-regularities’ (Lawson, 1997) are sufficient to reveal transfactual conditions. They are satisfied with corroboration as a measure of consistency, and believe that only reality is objective, or intransitive, and that our knowledge of it is not. Rather than the ‘verstehen’ sought by the constructivist, the realist seeks ‘erklaren’, research is therefore explanatory rather than appreciative in its approach to knowledge sought

Table 4 below summarises the Critical Realist response to the parallel criteria posed by Lincoln and Guba (1985)

	Empirical Quantitative Enquiry	**Naturalistic Qualitative Enquiry**	**Critical Realism**
Truth Value	Internal Validity	Credibility	Epistemic Fallacy
Applicability	External Validity Generalizability	Transferability	Demi-regularity Describe Transfactual Conditions
Consistency	Replicability	Dependability	Corroboration
Neutrality	Observer Objectivity	Confirmability Observed's objectivity	Intransitive objects of science
Knowledge sought	Seeks correlation	Seeks Verstehen	Seeks Erklaren

Table 4.4 Establishing Trustworthiness in Critical Realist Research

Seale (1999) further suggests that we should focus instead on whether the methods employed are appropriate to the question being asked, whether the selection of cases is theoretically justified, and whether the conclusions drawn follow from the data.

Outhwaite (1987: 58) suggests that findings as well as methods should be evaluated from a Critical Realist perspective. He suggests that

> "We shall …feel we have a good explanation if:

1. The postulated mechanism is capable of explaining the phenomena;
2. We have good reason to believe in its existence;
3. We cannot think of any equally good alternatives.

The Bounded Rational Model is capable of explaining Ethical Hacker decision making; we are able to understand the reasoning process in terms of the motivations, risks and bounds of behaviour. The regularity of the emergence of responses and the support from the literature gives us good reason to believe in the existence of the mechanisms described. As knowledge is transitive (Bhaskar, 1975) our challenge is to offer the best explanation that is possible, with the understanding that this may later be surpassed. Other writers at a later date may develop other explanations or may find evidence to offer further support to the model presented here.

4.5 Participants

Whilst it is necessary for the reader to have an understanding of the characteristics of the respondents, there is a need to protect the identities of those involved, many of whom admitted to being actively involved in criminality. These individuals, if identified, may see detrimental effects upon their own reputations and careers. This meant that the creation of individual profiles, by which individuals are highly identifiable, was not possible for ethical reasons. Instead, what follows is an overview of the characteristics of the group. There are clearly overlaps between the categories listed, however the protection of identities was essential, particularly in view of the fact that sampling was conducted through a system of referrals, which raised concerns among some of the respondents that the people that they introduced or were introduced by would recognise their profile.

There were a total of twenty-three respondents who were interviewed for this research. Of these twenty-two were male, all were between the ages of twenty and forty and all either worked in, or had previously worked in the field of Ethical Hacking, two had backgrounds in law, two were currently active police officers, two were educators. Of these, two individuals worked for themselves, freelance, and worked alone, two were Chief Executive Officers of large organisations and one was the owner of a large organisation, these therefore were involved in employing others. Four respondents were current students of ethical hacking, and seven were previous students.

4.6 Sampling

In order to be included in the sample to be studied, individuals self identified as being actively engaged in “Ethical Hacking”; this includes any activity that would normally be defined under the Computer Misuse Act of 1990 as being an offence, but where the activity is authorized and is therefore legal.

A purposeful sample was employed, using a ‘snowball’ technique to identify and access the sample. This technique makes use of the existing social networks of initial contacts to generate a population for research (Thompson, 1997).   The social networks utilised including personal acquaintances known to work within the field, and friends and colleagues of these who were recommended by respondents. Some respondents were identified by researchers and educators in the field who were able to identify some key informants, and also to make recommendations within professional roles including policing who may not have otherwise been accessible.

> Working with key informants means that you are attempting to gather some insider or expert knowledge that goes beyond the private experiences, beliefs and knowledge base of the individual you are talking to. Your goal is to find out what this individual believes 'others' think, or how 'others' behave, or what this individual thinks the realities of a particular situation might be.
>
> (O'Leary, 2004: 83)

Using key informants is a choice which fits within the Critical Realist approach. Extreme cases are selected over representative cases as "they often supply considerably more relevant information than representative or average cases" (Danermark, et al, 2002: 170). The respondents chosen represented a range of employees, employers and freelance workers, and ranged from students of Ethical Hacking, to those who were very experienced Ethical Hackers. This was in order to provide a 'snapshot ' of the field through a wide range of key informants in order to gain a broad understanding of the nature of the work, and the types of people involved. Extremely varied cases such as this are desirable within a Critical Realist framework as they allow us to "analyse how mechanisms operate under different conditions" (Danermark et al, 2002: 170)

The sample is purposeful in that the type of respondent desired was made known to the gatekeepers, who were the original contacts who identified further contacts, so that only appropriate respondents would be identified; appropriate respondents were those who currently or had previously engaged in using Hacking skills as part of their work.

This method of sampling is especially valid as Hackers share knowledge and information through a network of contacts (as described in Chapter Two). A purposive approach allows the selection of those who are best able to inform the study

(Cresswell, 2013). Snowballing has traditionally been utilised in sociological research for the purposes of accessing ‘reluctant’, or ‘hard to reach’ research populations, who may be difficult for the researcher to access because their behaviour is hidden. Those engaging in ‘Hacking’ would fit this category, as some of their behaviours were found to involve criminality.

The sample gradually builds during the research through a system of referrals from the initial contacts identified by myself and by educators and researchers working in computer security. Snowball sampling is often seen as a last resort and a solution to an access difficulty rather than an actual purposive choice. Researchers often use it because it is the only option and not because it is the best one. There are inherent problems with gatekeepers that may impact upon validity and can skew the sample by introducing other informants who will support their own views and opinions rather than giving a representative view of the field; however, the use of gatekeepers who are knowledgeable and who have access to ‘key informants’ can mean that a small sample can be especially representative, and therefore a relatively small sample that is carefully selected with the help of experts can reveal a wealth of data that is representative of the field.

The sample relies upon self-selection and recommendation, which risks bias. This sampling method is used when sampling frames are difficult or non existent and is reliant on introductions by people who are able to identify ‘good’ cases. The initial contacts act as gatekeepers to the other respondents and can therefore skew the typicality of the sample produced as they are only able to refer their associates, who may share there own views and opinions, or may be a limited range and therefore not representative of the field. In this sense the gatekeepers’ are best suited to identify potential research participant that may have otherwise been ‘hard to reach’.

Snowballing commenced from a range of already established contacts in order to reduce the negative ‘gate-keeper’ effects, (Whyte, 1955, Venkatesh, 1989) which is detrimental to the validity of the proposed research. The main difficulty with this is that the initial contact can influence the direction of the study by choosing later informants. The gatekeeper may present the researcher with a range of contacts who will support their own views rather than being representative of the population as a whole or may try to suggest informants who support the perceived desired outcomes of the research. Gatekeepers may also simply have limited contacts; they may not have contacts to whom the researcher may be introduced, or their contacts may be unwilling (Venkatesh, 1989; Bennett, 1997). Utilising a range of initial contacts reduced these negative impacts.

In addition to the above, an internet search for companies and individuals who offer Ethical Hacking services by advertising online, academic institutions and private companies that run degree programmes and training courses on Ethical Hacking produced a list of contacts that were contacted by mail and then followed up with phone calls making use of publicly accessible contact details, requesting an interview. This aimed to provide a wider contextual view of the development of Ethical Hacking and the Ethical Hacker, however, only one responded, and this was an educational professional who was interested in the research. He was able to act as a gatekeeper and provide referrals to professional in the field as well as some individuals who are currently studying Ethical Hacking and working in the industry in work placements. It may be that others chose not to reply because of the lack of reciprocity, in that there was nothing to gain for them in the research. They may also have had concerns about revelations of criminality, or concerns about privacy. Complete reliance upon snowballing has therefore maximized the gatekeeper effect and its associated limitations.

4.7 Ethical Considerations

There are a number of ethical issues which must be given special consideration in a study of this type, these are examined within the following section.

It was decided early on that it would be safer for the respondents, the researcher and the University if the respondents were Hackers who did not overtly partake in criminal activity, so, the focus was the ‘Ethical Hacker’ rather than the ‘Underground Hacker.’ Despite this, consideration was given in ethical planning to the potential that employed Hackers, may, in the course of their interviews intimate criminal activity that they were engaged in or were planning. In order to establish trust between the researcher and the respondent confidentiality is often offered.

> The efficacy of a research interview is largely dependant on the relationship established between the researcher and participant. It is important to create a rapport that facilitates the establishment of an atmosphere conducive to the disclosure of personal or sensitive information.”
>
> (Finch, 2001: 35)

However, there is often a conflict in conducting research between ethical and legal considerations (Finch, 2001). With this in mind it was decided that full confidentiality could not be offered, and that the circumstances under which confidentiality would not be upheld were clearly articulated to the participants. In the case of specific revelations with regard to criminal activity for which the respondent had not been convicted, or criminal activity which was being planned confidentiality was not assured, and it was made clear at the outset that the researcher would be obliged to pass information relating to harm or potential harm to the general population to the relevant authorities. Confidentiality was assured to respondents in so far as their personal opinions, and non-criminal behaviour.

> In terms of research into illegal activities, the purpose of interviewing those involved in committing crimes would be defeated if the research subject did not feel able to discuss anything connected with their offending for fear of prosecution
>
> (Finch, 2001: 36)

Respondents were advised that if they were to discuss any criminal activity it should either be activities that they had been convicted for already, or that specific details should not be revealed because "…it cannot be ethical to guarantee confidentiality that causes disclosure of information that the researcher has never been prepared to keep confidential" (Finch, 2001:43) This decision was made in order to protect the research participants from potential harms that would ensue from knowledge of any criminality being revealed to their employers or to the police because "it is of fundamental importance that no harm should accrue to the participants as a result of their involvement in research" (Finch, 2001 :48). This must however be balanced against legal obligation. Ethical guidelines from the British Society of Criminology further clarify the matter

> Offers of confidentiality may sometimes be overridden by law: researchers should therefore consider the circumstances in which they might be required to divulge information to legal or other authorities, and make such circumstances clear to participants when seeking their informed consent
>
> (British Society of Criminology, 2006)

Assurances of confidentiality were restricted in this way with the acknowledgement that this may limit the preparedness of the respondents to give full revelations of their behaviour. As the specific details of crimes committed were not the focus of this research this was deemed to be an acceptable compromise.

Potential harm to those engaging in research is also a consideration. One of the main characteristics that Hackers have in common is that they are curious, and often they do not trust outsiders. This means that any researcher going into this field is going to be subject to the investigations of those present. It was necessary to work with a computer security expert in planning the protection of both personal and research data.

An ethically significant risk to respondents resides in their need to protect their identity from other Hackers, and to protect their reputations within the security industry; guidelines regarding anonymity, confidentiality, privacy and data protection were adhered to.

In order to protect the respondents that data was anonymised, all identifying characteristics were removed, and the profile of the respondents within this chapter is presented as a group profile rather than a set of individual profiles.

The nature of the population to be researched led to some very significant risks, both for the researcher in terms of personal data security, but also for the university systems and networks. One possible solution considered was to set up a research group with no apparent affiliation to the University so that the University networks would be safe from attack; it was decided that this was not a practical option as it was too costly.

In addition guidance and approval was sought from The University of Northumbria Ethics Committee. The participants were asked for permission, and the procedures to be followed outlined. All subjects were over the age of 18, were fully informed about the aims and nature of the study, gave consent, and had the right to withdraw consent at any time.

The Association of Internet Researchers (AOIR, 2002) provides a useful guide to ethics in online social research. Although this research is not conducted online, the AOIR guidelines are appropriate because guidelines cover research that "studies large scale production, use, and regulation of the internet by governments, industries, corporations, and military forces" (AOIR, 2012: 4). In particular the AOIR (2012) make specific reference to the special care needed in data storage when dealing with internet research and online populations.

Because the respondents all have Hacking knowledge, and because their personal and professional reputations require protection in line with confidentiality agreements made, it was necessary to plan carefully to safely hold the data. Interviews were audio recorded; these audio recordings were stored on a laptop which is not used to connect to the internet, as were the verbatim transcriptions. This was password protected, and kept in a physically locked storage unit. These tapes and transcriptions were anonymised immediately after recording, and the list which identifies names to anonymisers was kept in a locked storage facility at another location.

4.8 Data Collection: Semi-structured Interviews

The main method employed for this research is the semi-structured interview. This method was selected because it allows for a conversational process, which includes some digression and elaborations, whilst also ensuring that the research questions are addressed. The use of the semi-structured interview means that the researcher uses a guideline as to the topics and questions that are to be discussed, but it also allows some flexibility within the method with regard to the questions asked, the order in which they are asked, and the particular wording that is employed.

Interviews have been carried out, with the aim of describing the personal histories of individuals who are currently, or have previously been engaged in ‘Ethical Hacking’. This choice of interview style provided subjective meaning, depth, and detail, as well as indicating the personal relevance structures of the respondents. Subjects provided a personal oral history relating to their engagement in Ethical Hacking and were asked to comment on their career, the nature and development of the sector, and their perceptions of the distinctions between the ‘Hacker’ and the ‘Ethical Hacker’.

Questions asked were not predetermined but rather were flexible and influenced by the psychological field of the researcher, for this reason it was important that the questions asked were related in some way to the narratives that were revealed. The ordering or wording of questions may for example produce very different results, the wording of questions therefore was designed to reflect the wording used by the respondents, and key terms were discussed and defined at the outset so that there was a shared understanding of what would be discussed, and this was framed by the respondents. The ordering of questions was not predetermined, but rather was guided by the respondents so that the interviews had a natural narrative flow. The responses and the flow of the questions are influenced by the frame of reference of both the researcher and the participant. The respondents may answer the same question very differently based on a number of factors, which either cannot be controlled, or are very difficult to control. These include the social characteristics and perceived relationship with the researcher, the environment the study is carried out within and the personal moods and feelings of the respondent.

The flexible nature of the questions asked, and the fluid nature of the aims of the study mean that the data gathered is not comparable, which some would suggest gives difficulty in the analysis of the data gathered, however it is acknowledged that "…all knowledge is partial, incomplete, and fallible" (Maxwell, 2012: 5). The knowledge revealed did however reflect the feelings and the knowledge of the respondents at the time of the interview, as they wished to reveal it to the researcher and so although reality may not be fully grasped, a certain level of reality, as the respondent chose to present it is revealed. The fact that reality cannot be fully revealed does not negate the importance of the reality that is revealed. The respondents give the researcher access to the empirical, which the researcher is able to utilize in formulating theories pertaining to the real (Danermark et al, 2002). The ethical hackers interviewed described their experiences; the researcher is then able to take an overview of the cases in order to identify the demi-regularities in the cases (Lawson, 1997; Bhaskar and Lawson, 1998) and the generative mechanisms which underlie the behaviour. These are outlined in chapters 5 and 6.

> For qualitative data collection (is) that data are usefully seen, not simply as 'texts' to be interpreted, or as the 'constructions' of participants (although they are this), but as evidence for a real phenomena and process […] that are not available for direct observation. (Maxwell, 2012: 103)

Mishler (1999) suggests that it is possible to utilize the narrative or conversational interview as a rich source of data while simultaneously having awareness, as a researcher, that the research process in itself will contribute to the construction of the narrative.

> …many researchers advocate a reflexive approach in which the role of the interviewer, relevant aspects of his or her own identity, and the details of the interaction between researched and researcher are understood as constituting an important part of the research evidence
>
> (Elliott, 2005:20)

The interview is "…not merely a tool of sociology, but a part of its very subject matter…" (Benney and Hughes, 1956:38) this however does not cancel out the usefulness of the approach as "…all knowledge is theory laden, but this does not contradict the existence of a real world to which the knowledge refers" (Maxwell, 2012: vii). Theories are "the transitive objects of science" (Danermark et al, 2002; 23), they can be surpassed by new theories however "reality exists and is what it is independently of our knowledge of it" (Danermark et al, 2002: 26). The aim is to produce the best theory possible based upon the empirical data available.

> "Qualitative interviewing is a way of uncovering and exploring the meaning that underpins people's lives."
>
> (Arksey and Knight, 1999:32)

The research questions have been addressed at different points within the interview. The reason for this is that the interviewee was in control of the narrative and so revealed the issues that they saw as being important to them, in the order and the style that they felt was appropriate to their narrative. The aim was to provide the respondents with an empowering interview experience that would allow them to act in their capacity as experts, and as key informants with regard to their field, in revealing to the researcher what they felt was relevant and was important. The respondent may not understand the phrasing or focus of the research question in the original academic jargon, so the questions needed to be phrased appropriately. Respondents also may not give the appropriate level of depth or detail to their responses to fully address the research question. For this reason, each research question has been operationalised by considering its possible indicators and producing a set of flexible questions that address the minutiae associated with uncovering the necessary data to fully address the research questions posed. These were only posed towards the end of the conversation if not already discussed by the respondents within their initial narrative. This flexibility has meant that questions were added, or amended as necessary during the interview to allow for a natural conversational flow. In addition this has ensured the production of narratives which are authentic to the respondent and which reveal what is of importance to them.

Personal interviews were audio recorded, with the consent of the respondents, in order to allow detailed transcription and increased reliability. This ensures accuracy in producing verbatim comments that were included in the writing up of the findings. All of the Interviews were carried out face to face in order to allow this audio recording, and also to help to establish a rapport between the researcher and the interviewee, which was found to help with the flow of the narratives produced.

There are a range of benefits to this type of research design. The method is high in validity as the respondent is provided with opportunities to give their viewpoints, feelings, and descriptions of behaviour. Complexities or ambiguities were clarified or further explored which may not have been possible with other methods of research. One of the key strengths of semi structures interviews is that there can be less prejudgment of what is and is not important as the interviewer allows the respondent to raise further issues for discussion.

Of course, all methodological approaches will also have limitations or flaws inherent within the design. Interviewing, particularly qualitative interviewing, is highly dependant upon the skill and the subjective knowledge of the researcher in both designing, and carrying out the interview The researcher in this case has prior experience of conducting qualitative interviews and field research, so was able to draw from this experience in order to conduct the interviews effectively. What was potentially more important is that the researcher showed interest and enthusiasm for the topic, which makes the respondents want to reveal their stories. The presence of the researcher and the involvement of the researcher in the design introduce interviewer bias which was kept to a minimum by ensuring that the respondents' narratives were invited right at the start of the interview, before any specific questions were asked, and that the specifics were related to comments that had been made by the respondents. The method is time consuming in terms of both data collection and analysis both of which are extremely complex, however it is during these important phases in the research that the key themes for analysis emerged. As a method, face to face interviewing can also be expensive – there are often travel and hospitality costs involved, but these costs are worthwhile as the data produced is so rich and meaningful to the respondents. Qualitative interviews have low reliability in that they cannot be replicated to produce the same findings, and they cannot be applied to a wider sampling frame, however reliability for the realist is to be found in the authenticity of the respondents, who were in this case all referred key informants, and experts in describing *their own* reality. Interviews can also produce invalid results, in that respondents may lie, or may misremember facts. This was not considered to be important as this still reveals reality *as the informant sees it*, or as they *wish it to be seen or revealed*. They may also have tried to rationalise (Sykes and Matza, 1957) their activities, and may describe different motivations than their original motivations in an attempt to‘re-do’ the event being described, even this is acceptable within this research, as this reveals much about what the respondent sees as being acceptable behaviour, and what factors make their behaviour and decisions more acceptable to themselves.

Detailed field notes were taken during the fieldwork stage of the research in order to enable some acknowledgement of the ongoing perceptions and choices made. A field journal is a useful addition to any research carried out ethnographically as it allows for the recording of seemingly unimportant details, as well as the thoughts and feelings of the researcher, which may later be important to the data analysis in order to have an understanding of how and the particular issues had emerged, and whether they belonged to the frame of reference of the researcher or the informant. The reflective field notes included any emerging themes and any new immanent or exmanent questions as they arose during the interviews and were used in a reflexive manner throughout the research process in order to review themes and questions arising from the data in a way that questioned assumptions and responded to ongoing findings.

4.9 Data Management Processes

There are a number of options available for data analysis including the production of typologies, or taxonomies, and processes of coding. In this research the data was transcribed verbatim, coded (open and axial) and also reduced, these processes are outlined below

Maxwell (2012) also describes the research process being a ‘reflexive process’ whereby the researcher often has to respond as new information emerges from interviews and how we then take this into consideration as we progress in the research process.

> [Reflexive analysis is] a process that requires you to: manage and organise your raw data; systematically code and enter your data: engage in reflective analysis appropriate for the data type: interpret meaning, uncover and discover findings: and, finally, draw relevant conclusions, all the while being sure to keep an overall sense of the project that has you consistently moving between your data and your research questions, aims and objectives, theoretical underpinnings, and methodological constraints.
>
> (O’Leary, 2004:185).

The first stage of the data analysis was verbatim transcription, during this task, the researcher began to interpret the data collected by engaging with it through coding, memoing, and thick description. Verbatim transcription took about 3-4 hours per hour of recording. This can take longer where other details such as intonation, gesturing, laughing etc which can be important as they may reveal how the respondent feels about what they are saying. These were only included when they seemed particularly significant to elucidate what was being said, in particular, pauses were noted as they revealed that the respondent was hesitant to share some key information, or that they were unsure about what they were saying.

The second stage is to condense this into summary sentences, and finally to condense this again into key words and phrases. This progressive reduction in the data is clearly qualitative in nature, and therefore required some level of interpretive analysis by the researcher when employed. Each stage of data reduction reduces the validity of the data further as the influence of the interviewee is reduced and replaced by the subjective judgment of the interviewer as to which pieces of information are of importance. This method of analysis is employed in order to identify key themes emerging from the interviews (an approach advocated by Riessman, 2008). This data reduction was only employed in order to provide key themes that were of use in presenting the data. The emergent themes were the nature of Hacking and Ethical Hacking, communities and social structures, employability, education, criminality, and notions of right and wrong. As this data reduction is heavily reliant on the perspective of the researcher, open and axial coding of the whole transcripts were also employed, in case any issues of importance to the research had been overlooked.

The other mode of analysis employed was the use of open and axial coding. The choice was made to analyse the data using a process of verbatim transcription, open, and then axial coding, along with memoing and description. Open coding is “breaking down, examining, comparing, conceptualising and categorizing data” (Strauss and Corbin, 2007:61). “A code is a summarizing piece of phrase for a piece of text which expresses the meaning of the fragment” (Boeije, 2010: 96). Open coding has been completed at the interview transcription stage in order to “…examine the text for salient categories of information” (Cresswell, 2013: 1995).

Open coding was carried out with highlighters and post-it notes, due to the researcher’s preference for a ‘hands on’ approach, although this may also be also be carried out using computer programmes. Central themes which were repeated throughout the interviews were revealed, along with certain themes that were particularly important to the respondents as they were prominent within the interviews. It was at this stage that the defining factors in decision making were identified.

This process was followed with axial coding to elucidate on these central themes and the addition of any new questions taking place after the initial transcription and coding had been completed. Axial coding is "…a set of procedures whereby data are put back together in new ways after open coding, by making connections between categories" (Strauss and Corbin, 2007: 96). "The relationships between salient categories (axes!) and subcategories can be generated, moderated, elaborated, or even rejected throughout axial coding" (Boeije, 2010: 96). Axial coding allows for the addition of new codes if any are missing, new connections to be made between the categories, and categories that are not useful to be removed. It was at this stage within the research that the choice was made to include the idea of rationality being bounded (Simon, 1957; Clarke and Cornish, 1985; Cornish and Clarke, 1986; Gigerenzer and Selton, 2001; Selton, 2001; Cornish and Clarke, 2008).

The researcher will always influence the choice of labels applied in open coding, and the categories and clusters created in axial coding are subjective and will be influenced by exmanent issues such as the research questions, or researchers own interests, and the frame of reference of the person framing the questions. For this reason, the codes that emerged were regularly reviewed and amended, particularly as it may be viewed as unethical to use codes or labels that the respondent does not advocate or embrace (Weis and Fine, 2003). Cresswell (2013) calls this approach "emergent design", the design is flexible and responsive to new knowledge gained during the process.

Later respondents in the study were asked to comment upon these emerging themes, in order to see if they felt that the field was being revealed in a way that was true to their experience.

After the research was analysed and written up the original interview recordings were listened to again, this proved to be revealing, as once the key themes had been selected and organised details which had been previously overlooked proved to be salient.

4.10 Interpretation and Presentation of Findings

The use of the 'Bounded Rational Model' (which is discussed at length in section 5.2) of decision making means that the data is presented in a way that reveals the issues that influence the decisions that are made by the respondents about whether to be involved in criminality and whether to engage in Ethical Hacking as a career, and also about individual criminal events.

The following chapters will therefore discuss what it means to be a hacker or an ethical hacker in the perception of the respondents, followed by the impact of employability and the growth of the sector, education and its impacts, and the decisions that are made by employers. This discussion is to be found within Chapter Five.

Following this is a detailed examination of decisions regarding 'right' and 'wrong' behaviour, which includes a detailed discussion of both normative and meta-ethical approached to decision making. The motivations, heuristics and other boundaries to decision making are considered throughout. (Please see Chapter Six for a further discussion).

4.11 Summary and Conclusions

The decision was made to conduct in-depth interviews with the specific group of Hackers to be studied. The interviews were semi structured and encouraged as much narrative as possible from the respondent in order to reduce the impact of the interviewer and to create authenticity. The respondents were invited to reveal their personal narratives by the use of open questions, and prompting and questions were kept to a minimum.

The data was analysed making use of open and axial coding, and data reduction in order to reveal and organise key themes.

The study is distinct and creates an original contribution to knowledge by offering an exploration of a newly emergent and still developing social group. An examination of this group may add a new category to those already established and accepted typologies extant within the available literature as Ethical Hackers have been found to be qualitatively different to their Underground hacker counterparts. The research provides potential to develop an understanding of the life course, motivations, relationships and practices of the Ethical Hacker and the social world in which he operates. This is examined through the lens of bounded rational decision making (Simon, 1957; Clarke and Cornish, 1985; Cornish and Clarke, 1986; Gigerenzer and Selton, 2001; Selton, 2001; Cornish and Clarke, 2008).

The methodological framework allows for a detailed examination of the personal journey made by computer Hackers explaining how and why they choose to become contracted or salaried to provide security solutions to business, industry and law enforcement in return for fees and salaries rather than acting illegally. It is of interest that many choose to continue to act illegally – the decision making processes behind this are examined.

Critical realism was adopted as "…realism helps to resolve some of the serious philosophical, theoretical and methodological problems that qualitative researchers face", It has allowed "…a commitment to the existence of a real though not an objectively knowable world" (Maxwell, 2012: ix).

Chapter 5: Theorising Ethical Hackers

"…to be an Ethical Hacker is a breeze, but there is so much more to Hacking"

(Respondent 9)

5.1 Introduction

The aim of this Chapter is to consider what it is to be an 'Ethical Hacker'. In order to achieve this, respondents views on Hacking, Ethical Hacking and employability in the sector are discussed as well as how and why they entered the field. The employability of those with criminal or underground backgrounds or affiliations, and why those who switch from underground Hacking to Ethical Hacking do so will all be discussed within this Chapter.

There would appear to be a number of similarities between Hacking and Ethical Hacking which are evidenced in the responses of those interviewed. There are also some distinguishing features, as well as some commonalities to be examined. In order to gain an understanding of these, the following sections will consider the nature of Hacking and of Ethical Hacking, and what distinctive and overlapping features exist.

There is a broad range of academic and scholarly literature which focuses upon the history of Hacking and typologies of Hackers. There is a clear gap in the literature, an omission with regards to the nature and development of Ethical Hacking, which has only recently begun to be discussed in the literature, and on which only limited research is currently available.

Hackers have come to be understood through a range of typologies (though these often conflict) through their social organisation (which provides a community, and a network of support) and through the hierarchical power structures which define these communities and are based upon knowledge and skill. Ethical Hackers have not previously been examined in relation to motivations, community or power structures.

While a range of criminological theories are applicable to underground Hacking, the Ethical Hacker does not seem to fit neatly within the typologies created by criminologists. As this research shows, the Ethical Hacker can be understood with relation to his socialization, his views on ‘right’ and ‘wrong’, his professional conduct, and his relationship with the wider Hacking and Ethical Hacking communities. The difficulty which arises with solely relying upon criminological theory is that different theories seem to explain different types and aspects of hacking behaviour, so that no theory is applicable to all, and also that Ethical hacking is not typically associated with criminality. Alternative theorising is therefore necessary.

Bounded Rational Choice (Simon, 1957; Clarke and Cornish, 1985; Cornish and Clarke, 1986; Gigerenzer and Selton, 2001; Selton, 2001; Cornish and Clarke, 2008) will be used as a model for understanding the decisions and behaviours of Ethical Hackers, with an awareness that “The glasses one wears magnify one set of factors rather than another” (Allison and Zelikow, 1999: 387). The reason for this choice is that it explains the decisions and behaviours of Ethical hackers (and other types of behaviour) in a way that allows us to examine the motivations, behaviour, decisions and community of the Ethical Hacker in a way that allows us to explain criminal events and criminal involvement or non-involvement, while acknowledging the structural, personal and heuristic boundaries that limit the reasoning of the Ethical Hacker.

> …models of bounded rationality describe how a judgment or decision is reached (that is, the heuristic processes or proximal mechanisms) rather than merely the outcome of the decision, and they describe the class of environments in which these heuristics will succeed or fail. These models dispense with the fiction of optimization, which in many real-world situations demands unrealistic assumptions about the knowledge, time, attention, and other resources available to humans.
>
> (Gigerenzer and Selton, 2001: 4)

The following section will discuss the development of the model used by outlining the useful parts of game theory from within the economic Rational Actor model, and from within criminological Rational Choice Theory. The discussion will evaluate these approaches in order to show how and why the bounded model is arrived at. The model then is clearly defined at the end of the section.

5.2 Bounded Rational Choice as a model for understanding Ethical Hacker decision making

There have been some attempts to use game theoretic modelling in the study of criminal Hackers, (for example see Moayedi and Azgomi, 2011) however the mathematical modelling is an attempt to quantify a set of factors and variables which can only be understood qualitatively. Game theory is a division of decision theory whereby strategic interactions between rational actors create outcomes which reflect the interplay of their preferences and the strategies employed. Game Theory sees the individual actors as making decisions by means of a costs-versus-benefits analysis, where the decider weighs up the inputs and the potential outcomes of a decision or an action. In modelling how decisions are made, game theorists attach numerical values to these factors and create equations which can calculate the outputs of decisions

(Shim, Allodi, and Massacci, 2012). Game Theory has been made use of in economics, in the political sciences and in research which explores consumer behaviour. Whilst the ideas and concepts used in game theoretic modelling are of use within this research, the mathematical modelling is problematic as the inputs and outputs are subjective, and the variables involved are affected by the individual frames of reference of the people involved. Moayedi and Azgomi (2011) point out that the diversity in Hacker types makes game theoretic modelling particularly difficult. “If there is a large set of Hackers, the game model cannot be solved easily” (Moayedi and Azgomi, 2011: 46).

Although the “game model cannot be resolved easily” (Moayedi and Azgomi, 2011: 46) the reasoning process that is described is useful in developing a framework for understanding choices that are made by Ethical Hackers. Of particular use is the idea of the choice between legal or illegal behaviours being a rational one, in which the decider engages in reasoning, and attempts to optimise, or maximise the potential outcomes.

> During an attack process, a Hacker chooses an action among a set of different possible actions at each internal step of the process. Likewise the system administrator may arrange plans to thwart the attack. Each decision made by these two opponents follows a rich set of properties of its performer such as: motivation, skills, possibilities and the current amount of knowledge about the system
>
> (Moayedi and Azgomi, 2011: 45)

Traditionally, Game Theory is a quantitative approach, which gives numerical values to the inputs and outputs in any decision. While the concepts and ideas provide a useful framework for understanding decision making processes, the mathematical modelling is at best problematic, in that the values of the various inputs and outputs are subjective and therefore do not lend themselves easily to quantitative measurement. In addition they “do not consider the large number of Hackers and the diversity in their behaviours” (Moayedi and Azgomi, 2011: 46) or the “incomplete knowledge of players about the games rules, the other players’ possibilities, and the overall game” (Moayedi and Azgomi, 2011: 45).

While traditional Game Theory, with its roots in economic evaluations and mathematical modelling may not be fully applicable, the Hacker is faced with “… an array of potentially effective strategic alternatives” (Shim, Allodi, and Massacci, 2012: 1) thus suggesting that an understanding of the Hacker through a rational model is useful, while traditional Game Theory does not capture the intrinsic qualitative nature of these human decisions and interactions. The Hacker “...faces uncertain situations and needs to make a choice from a set of available actions. Each of these actions has a different probability of yielding an outcome” (Shim, Allodi, and Massacci, 2012: 3); these probabilities are inherently unknowable. The decision maker may be aware of the likelihood of improving or worsening the situation but is unlikely to make a quantitative analysis of this:

> Boundedly rational decision makers do not necessarily form quantitative expectations. Instead, they may rely on qualitative expectations connected to decision alternatives. This means that the decision maker has expectations about the direction of change compared with the present state of affairs.
>
> (Selton, 2001: 21)

Clarke and Cornish (2000) would suggest that the offender is a reasoning and rational individual. He will weigh up the relative positive and negative outcomes associated with a course of action and will make an effective decision. Crime is not expressed in mathematical terms within Rational Choice Theory, rather it is expressed through decision diagrams (Clarke and Cornish, 1985; Cornish and Clarke, 1986). The theory suggests that crime may be controlled by reducing the positive sanctions (rewards) and increasing the negative sanctions (punishments). Rational Choice theory advocates for separate decision analyses to be carried out for different types of crime (Clarke and Felson, 1993: 6) as these will have different actors, different motivational factors, and different sets of constraints. "The rational choice perspective sees the nature of the crime committed as crucial to explanation, since the decisions leading to one type of crime are different to those leading to another" (Clarke and Felson, 1993: 6)

This approach is an important ingredient in the analysis of decisions made by Ethical Hackers because hackers have been found to:

> …have a considerably higher need for cognition and higher risk propensity than the general public. They tend to prefer rational thinking styles over intuitive approaches and they demonstrate a particularly high confidence in their ability to reach optimal decisions through a rational deliberation process
>
> (Bachmann, 2010: 652)

Rational choice as a framework for understanding decisions assumes that a problem can always be separated from other problems. Individually rational decisions may not always produce a rational outcome.

Bounded rationality within Rational Choice theory is understood as being optimisation within constraints. Decision-making is inhibited by environmental or 'situational' factors, including time, cognitive ability, and the level of obtainable information; this results in a 'bounded' rationality rather than total rationality (Cornish and Clarke, 2008).

This however, is not the only sense in which bounded rationality is understood.

> Bounded rationality is neither optimization nor irrationality. Nevertheless, a class of models known as *optimization under constraints* is referred to in the literature as "bounded rationality," and a class of empirical demonstrations of

> so-called errors and fallacies in judgment and decision making has also been labeled "bounded rationality." The fact that these two classes of models have little if anything in common reveals the distortion the concept of bounded rationality has suffered.
>
> (Gigerenzer and Selton, 2001:4)

The other forms that will be discussed include satisficing, which is making do with a less than optimum, but acceptable option (Simon, 1957).

> Most human decision making, whether individual or organizational, is concerned with the discovery and selection of satisfactory alternatives; only in exceptional cases is it concerned with the discovery and selection of optimal alternatives.
>
> (Simon, 1997: 140-141)

The importance of Simon's concept of satisficing is discussed by Selton (2001) who suggests that as well as the process of satisficing, what the individual is attempting to chief is of significance:

> Often, satisficing is seen as the essence of Simon's approach. However, there is more to it than just satisficing. Aspiration levels are not permanently fixed but are rather dynamically adjusted to the situation. They are raised if it is easy to find satisfactory alternatives, and lowered if satisfactory alternatives are hard to acquire. This adaptation of aspiration levels is a central idea in Simon's early writings on bounded rationality.
>
> (Selton, 2001: 14)

As well as situational factors and satisficing, rationality is also bounded by heuristics, which are guidelines for how to act in specific circumstances. The inclusion of these boundaries deals with one of the main criticisms of Rational Choice Theory as identified by Blau (1997):

> Rational Choice Theory is often criticized for explaining individual behavior in purely rational terms. The gist of this criticism is that the theory ignores nonrational human behavior, neglecting such influences on it as emotional, pathological, and moral (normative) ones.
>
> (Blau, 1997: 16)

Bounded rationality acknowledges emotional, pathological and moral constraints on decision making.

This does not mean, however that we will dispense entirely with the Criminological Rational Choice Theory (Clarke and Cornish, 1985; Cornish and Clarke, 1986; Cornish and Clarke, 2008), it will be used alongside the concept of Bounded Rationality (Simon, 1957; Gigerenzer and Selton, 2001; Selton, 2001) as reason bounded by satisficing (Simon, 1957) and heuristics, as it allows us to examine a different set of constraints which will compliment the model, but also allows for the Criminological framework of events and involvement decisions to be considered. Rational Choice Theory (Clarke and Cornish, 1985; Cornish and Clarke, 1986;; Cornish and Clarke, 2008) deals with optimisation under constraints rather than heuristics (Gigerenzer and selton, 2001; Selton, 2001) and satisficing (Simon, 1957) as the key boundaries to reasoning. This research will include both conceptualisations because both are useful to us in understanding the Ethical Hacker. According to the theory decisions are made differently with regard to whether they are decisions about criminal involvement or are criminal events:

> Involvement decisions are characteristically multistage, extend over substantial periods of time, and will draw upon a large range of information, not all of which will be directly related to the crimes themselves. Event decisions on the other hand are frequently shorter processes, utilizing more circumscribed information largely relating to immediate circumstances and situations
>
> (Cornish and Clarke, 1986: 2)

Rational Choice Theory has been criticised because criminality does not always produce rational outcomes, and does not always consider all of the possible options or inputs, in fact criminal often have a limited ability to generate or to search for alternative courses of action. Rational Choice Theory and Bounded Rational Models acknowledge these issues, they do not expect ‘full’ rationality:

> Full rationality requires unlimited cognitive capabilities. Fully rational man is a mythical hero who knows the solutions to all mathematical problems and can immediately perform all computations, regardless of how difficult they are. Human beings are in reality very different. Their cognitive capabilities are quite limited. For this reason alone, the decision-making behavior of human beings cannot conform to the ideal of full rationality.
>
> (Selton, 2001: 14)

If a decision maker was fully rational, they would have full information, know all of the alternatives choices, understand all of the consequences, and would establish a scale of outcome preference. The outcome would also always be the most effective or efficient. The decider may not always actually have all of the available choices available to them as choices:

> A country's economic development, stage of technology, and its labor force's occupational distribution, for example, govern the opportunities for successful careers and social mobility. Hence, these structural conditions govern the rates or probabilities of realizing career aspirations in the population.
>
> (Blau, 1997: 17)

Having a criminal record will severely restrict the ability of the Hacker to decide to go straight, even though given the diminishing rewards of criminal behaviour, and the increased rewards and reduced risk involved in Ethical Hacking this may appear to be the optimum course of action. This illustrates the bounded nature of the reasoning that we will observe among Ethical Hackers within this chapter and within chapter 6.

The Bounded Rational Model that is employed in this research combines criminological ‘Rational Choice Theory’ and The Economic ‘Rational Actor Model’, whilst considering the criticisms of both perspectives, as outlined above.

The Bounded Rational Model sees decisions made by a process of reasoning, whereby individuals seek to increase positive outcomes, and decrease negative outcomes. Optimisation is restricted by heuristics, satisficing and situational factors.

5.4 The Ethical Hackers' View of Hacking

The interviews carried out commenced with a discussion around what it means to be a 'Hacker'. This was in order to establish a common frame of reference given the range of different definitions of the words 'Hacking' and 'Hack'

Those interviewed generally did not define 'Hacking' as being an activity, but rather described it as a way of thinking, as a general approach to solving problems, or a set of motivations. Some did refer to it distinctly as an activity, and where this happened it was described as a criminal or deviant activity (see also Parker, 1998; Taylor, 2000; Wall, 2007), with respondents making statements such as: "…very simply Hacking is, I see it as, being a criminal activity" (Respondent 16).

However these absolute views of the hacker as a criminal were rare; they were strictly confined to, although not representative of, those from law enforcement rather than from underground backgrounds. Those with underground affiliations did not tend to perceive legality as being a defining issue in the nature of Ethical Hacking or Hacking, but rather made personal choices about whether they perceived a specific action to be 'right' or 'wrong' in relation to the level harm that they perceived to be the outcome of their actions.

Bounded Rational Models (Simon, 1957; Clarke and Cornish, 1985; Cornish and Clarke, 1986; Gigerenzer and Selton, 2001; Selton, 2001; Cornish and Clarke, 2008) have been criticised for not taking into account the social, and for focusing instead only on individual outcomes of decisions (Blau, 1997). As we shall see within this chapter and also within the next one, the respondents did sometimes take into account harm to others when making their decisions (or they at least rationalised their behaviour after the fact in these terms (see Sykes and Matza, 1957 on denial of injury as discussed in Chapter Three), which means that the Bounded Rational Model must therefore be understood as a being a social as well as a psychological theory. The following statement is illustrative of this point:

> …it is not a game, because people lose money, and people go out of business. We have instances that we have dealt with where the machine has been crashed, and the company has said we just can't function any more so we are not going to, so then for people to say well there was a weakness and therefore I did it does not justify it for the people who have lost their jobs, and as I say, this is the attitude that I have to it, is that those people should be prosecuted, although it is a very difficult crime to prosecute
>
> (Respondent 23)

A number of the respondents saw Hacking as being something which can be either legal or illegal. One respondent commented that he was "…totally happy to use the term Hacker for legal activity, [laughs] yeah, [laughs] especially for legal…" (Respondent 9).

The understanding of Hacking as being unrelated to legality is found to be a common perception among the computer underground generally, and specifically within the FOSS community. Early conceptions of Hacking, precriminalization shared this understanding (Levy, 1984, Taylor, 2000).

Prevalent among the respondents was the idea that being a Hacker is about being talented, being gifted, having skills, and having a passion for what you do. According to the respondents to this study these characteristics are not found in all Ethical Hackers, with the implication that this may mean that not all ‘Ethical Hackers’ are ‘Hackers’. One respondent stated that in his opinion “…being a Hacker is about knowing, and being technical, and being skilled at what you do as far as computing and networks and applications…” (Respondent 2). There would appear to be some similarities between Ethical Hacking and Hacking however; respondents consistently suggested that “…they [Hackers and Ethical Hackers] are two distinct groups. The common ground is the tools that they use and the techniques that they use; though not the skill, but the tools” (Respondent 1).

It would therefore appear that being a Hacker is perceived to be more closely associated with your level of ability than any particular activity you engage in, or any individual specific act, even where the same tools and techniques are made use of. Self defined ‘Hackers’ tended to describe themselves in terms of their motivations as well as their skills, with the two often being intertwined. Respondent 3 said that he “want[s] to see if [he] can do it, for whatever reason, for personal gain, or for actually trying to build up [his] skills” (Respondent 3). He clearly indicates here some of the perceived gains which affect his reasoning in deciding to Hack; he engages in Hacking based upon the benefits that he perceives he will gain from the activity, which would support the idea that there is a reasoning and rational process which is involved the decision to Hack. Respondent 3 is here indicating optimising behaviour, through weighing up what he can gain from his actions.

Respondent 9 was particularly emphatic about the relationship between the level of skill that an individual has and the perception of them as being a Hacker; he returned to this point at several instances within the interviews. He states that:

> I think it [Hacker] is quite a positive term…its not like once you are a Hacker you are going to go and steal something…I believe that its something more,.. more about the skills that you have not something that is more about the stuff that you do.
>
> (Respondent 9)

He later goes on to elaborate on this point by saying that the Hacker:

> …is not really somebody who gains unauthorised access, he is somebody who is technically skilled, who can write exploit code, whether to distribute, or to keep it for themselves. It is someone who really, really has a very deep knowledge of computers, networks, and everything else concerned with that really.
>
> (Respondent 9)

What defines Hacking then is the knowledge and skill which underlies it rather than the actions that are carried out, so that is necessary to understand the action as being informed by the history, knowledge and development of the actor. This personal history, knowledge and understanding must be understood as bounding the rationality of decisions that are made by providing a frame of reference and a set of social norms from within which the Ethical Hacker, or the Hacker will decide how to act. Whilst there is a process of reasoning, and weighing up the possible costs and benefits associated with a course of action, these boundaries can limit the rationality of the outcome of decisions that are made (Simon, 1957; Clarke and Cornish, 1985; Cornish and Clarke, 1986; Gigerenzer and Selton, 2001; Selton, 2001; Cornish and Clarke, 2008).

Even those who did not and had never engaged in illegal Hacking could understand challenge as a motivation in Hacking. One public sector worker in computer forensics commented that he could "…see where the challenge is in doing that" (Respondent 5). One respondent in this research stated that in his opinion "…a lot of those guys [Hackers] do it just for a challenge, or just to prove they can…they are not really out to cause any harm, or do any damage or anything, it is just to prove something."(Respondent 8) so that we can understand as challenge and status as being intrinsically linked.

Hackers are thought to be particularly driven by challenge, and in particular challenges which require cognitive skill (Dalal and Sharma, 2007; Holt and Kilger, 2008; Schell and Melnychuk, 2010) and this therefore offers much more significant rewards to them than is apparent in the wider population (Bachmann, 2010).

> They are eager to learn about the technical intricacies of systems and processes, enjoy exploring their details and thrive on mastering the intellectual challenges involved in altering or circumventing their functions and limitations.
> (Bachmann, 2010:644)

Many other respondents reinforced the elements of passion, "… you need to be quite passionate about Hacking …You need that drive, you need that focus [pauses] erm [pauses] you need to love what you do as well" (Respondent 9) drive, "You've got to want to be a Hacker…… I think there is a lot more work being involved in being a Hacker than there is being a penetration tester…"(Respondent 6) and talent and ability as being the key defining factors in Hacking, "You need to be quite gifted in what you do to be a Hacker; I personally think you need to be quite gifted…" (Respondent 2). Hacking would therefore appear to be less about *what* you do, and more about who you are, and *how* and *why* you do it.

Alongside these suggestions that Hacking is about having passion, drive, talent and ability, there were statements which suggested that there was also the need to gain status with other members of the hacking community as a common motivational factor. For example, one commented that “Generally when you get a group of Hackers together in the same place its just sort of like bragging rights.” (Respondent 19). It was common for the respondents to describe Hackers as being proud of their achievements, and suggested that it is common for them to share their experiences with others in order to impress other members of the community

This seems to be only acceptable within the Hacking or Ethical communities, and not within other social networks that the individuals may be engaged in. “You want to be able to say I have done this and I have done that [but] It is not something that you would mention if you were out for a drink in the town” (Respondent 22).

These comments suggest that Hackers restrict where and when they share information about their activities, and that they restrict it to times and to people that they see as being appropriate. This may increase the motivation to move from Hacking to Ethical Hacking, as the activity becomes more socially acceptable and therefore the information relating to behaviour can be more widely shared within society.

This trying to gain status and to impress others includes Hackers who feel that they need to be better than those working in security as a way of ascertaining and proving their abilities:

> “A lot of Hackers just do it to prove that they are better than the guy who secured the system.”
>
> (Respondent 18)

As well as Hackers trying to contend with security, Ethical Hackers are trying to compete against Hackers so that it comes to be perceived by some as being "…a game, a challenge, you are trying to win one over, trying to secure things just for the sake of making things more secure…" (Respondent 15). This is necessary because Hackers are "…changing their tactics all of the time… it is that thing of trying to be one step ahead…" (Respondent 7). This game, in which both players can be seen to make rational, yet bounded series of decisions, is described by Moayedi and Azgomi, (2011) in their framework for analysing the impact of hacking diversity in the design of security measures:

> During an attack process a hacker chooses an action among a set of different possible actions at each internal step of the process. Likewise the system administrator may arrange some plans to thwart the attack. Each decision made by these two opponents follows a rich set of properties of its performer such as: motivation, skills, possibilities and the current amount of knowledge about the system.
>
> (Moayedi and Azgomi, 2011: 45)

This means that the nature of Hacking is understood to involve having ability, but also it is seen as being essential that people are made aware that you have that ability. The level of ability is proven to the self and to others through competition between individuals in a kind of game. Hacking is clearly, in the views of these respondents, related closely to the status that it carries with others. "…a lot of Hacking at the minute is just to prove a point and if you want to prove a point you want people to know that you have proved this point" (Respondent 22). Therefore, the decision to be involved with Hacking has a clearly social as well as an individual element to it. If an activity can gain status, or can give the individual a sense of 'winning the game' then this clearly adds something to the perceived gains, or benefits that will be derived from the activity. For both Hackers and Ethical Hackers this would appear to be a significant motivational factor.

Hackers are known to be driven by the desire to learn and to explore (Denning, 1990). If we see the Hacker as being someone who is driven by the challenge of finding things out (Denning, 1990; Stouffer et al, 2011), and learning new skills, then it comes to be apparent that some of the Ethical Hackers and some of the Underground Hackers can be defined as being Hackers, but that the term is not completely synonymous with either Ethical Hacking or Underground Hacking.

It would appear from the responses given that the intrinsic challenge is something that Ethical Hackers are driven by and that it is something that they constantly seek, requiring them to search out new activities to rejuvenate the sense of satisfaction that they receive from their behaviour. There is a clear element of diminishing personal rewards as repeated behaviour will make it less challenging each time, thus meaning that Hackers constantly strive for new sources of self-realisation and may engage in new, different, or more difficult hacking activities because of this. In order to ensure desistence the Hacker must be understood as being rational because research has indicated that "…directly reducing the returns from malicious activities is the only effective strategy for hackers both with a low-medium skill, and with a high skill" (Shim, Allodi, and Massacci, 2012: 1).

A reasoning individual may alter the decisions that they make as part of a cost versus benefit analysis (Simon, 1957; Clarke and Cornish, 1985; Cornish and Clarke, 1986; Gigerenzer and Selton, 2001; Selton, 2001; Cornish and Clarke, 2008) where the rewards have diminished this may suggest to the actor that a different course of action is in fact more reasonable for them, as it will provide greater rewards. A more challenging target will present greater rewards if challenge is a significant motivational factor.

The idea of gaining personal rewards through being challenged came up frequently within the interviews, which is indicative that this is of importance in the mind-set of an Ethical Hacker. Hackers are described as being "…problem solvers…challenge is at the bottom of all Hacking in my opinion" (Respondent 2).

This idea of challenge as motivation is described in relation to the wider Hacking community by Cornwall (1985: 1), who sees the *process* of Hacking as being intrinsically more important to the individuals who engage in it than the outcomes that it produces, stating that "…the process of 'getting in' is much more satisfying than what is discovered in the protected computer files". If we are to consider a cost benefit analysis within decision making, it would seem to be apparent that the thrill gained from rising to such a challenge must be considered to be a positive output, and therefore an outcome in itself, rather than simply just considering the outcome of the Hack in terms of gaining access, "…they are…thrill seekers who derive pleasure and excitement from the chase, from overcoming barriers, from gaining access to other systems" (Bachmann, 2010: 64).

Hackers being driven by the challenge involved may go some way toward explaining why they decide to change careers or 'hats'. They do this in order to provide diversity in the kinds of activities that they are able engage in, this explaining why some move from Underground Hacking to Ethical Hacking. As exploits have largely come to be publicly accessible on the internet, the challenge is no longer there for the individual in engaging in with criminal behaviour and therefore the risk and the rewards are both reduced. “It is as easy as typing five or six more numbers on your web browser to get all those credit cards. That is how easy it is” (Respondent 2).

It may be assumed that the move into crime prevention provides greater rewards for the individual as it can be more challenging, not necessarily in that it is more difficult to do, but that it can provide variety in the types of challenge and adversary. There is also a fee or a salary included as a motivational factor in being employed. The legitimate face of Ethical Hacking also allows for bragging to extend outside of the community and into wider society where illegal hacking may have been perceived to be unacceptable, but where being employed using hacking skills can hold status because these skills are not widely held or understood. As we have seen, bragging is common and status is described as a significant motivational factor for the respondents in this study so this may also increase the perceived benefits in switching career. Ethical Hacking has reduced costs as compared to Hacking in that the risk of prosecution is removed or is otherwise significantly reduced, and therefore the rational model alongside an understanding of challenge as motivation helps us to explain desistence behaviours among Hackers, who actively make the choice to move into a legitimate career.

If we understand the nature of Hacking as being informed by the Bounded Rational Decision Model (Simon, 1957; Clarke and Cornish, 1985; Cornish and Clarke, 1986; Gigerenzer and Selton, 2001; Selton; 2001; Cornish and Clarke, 2008) it may be that we come to see this ‘hat switching’ as being *a change in strategy within a game*, or as *being a change in team, but within the same game*.

As we will examine further, it may be the case that the challenge as motivation thesis may also explain why many of the respondents see Hacking and Ethical Hacking as connected and interdependent activities, with the skills from each area providing advancement in the other.

5.4 Are ‘Ethical Hackers’ ‘Hackers’?

Many of the respondents focused on the similarities that they perceived between Hacking and Ethical Hacking when asked to provide definitions, seeing these as being similar or overlapping activities. As previously acknowledged, when asked to define how they perceive the nature of Hacking, the respondents tended not to define it as being an activity. When hacking was talked about in this way, the discussion of it as being an activity shows that the respondents do in fact describe both Hacking and Ethical Hacking as being activities when asked to differentiate between the two. They may not define it as an activity when asked directly, but the wording and the descriptions that they used when comparing the two in this way indicates that they may see it as an activity, even though they may not be aware that they do, and not directly describing it in this way. For example Ethical Hacking is described as being “…much the same as Hacking, using the same sort of tools, you’ve got the same outcome, but you are doing it under contractual obligation.” (Respondent 22)

The respondents revealed that often the activity that they are describing is the same for both Hackers and Ethical Hackers, they see both as the circumvention of software, with the difference between the two lying in the context and in whether authorisation has been gained. Ethical Hackers described that their work included doing "…what the average Hacker would do" (Respondent 8) and that they perceived that there are "…similar skills between being a Hacker and an Ethical Hacker, but [with] different end points" (Respondent 20).

The outcome of Hacking and of Ethical Hacking therefore is perceived as being somehow different. The motivation may also be different, as described by respondent one when he describes his perception of Ethical Hacking behaviour. Ethical Hackers are, in his perception:

> …people who have the knowledge and skills to Hack, but do not cause any damage, it is a moral choice. They do not have any contractual obligation other then their own morals. People who are hired are doing it for a pay check.
>
> (Respondent 1)

Respondent one seems to be implying here that he feels that true ethical behaviour is engaged in for an ethical purpose or should not be described as being ethical. The person who is hired or employed as a so called Ethical Hacker, is not 'ethical' as they are financially rather than ethically motivated. So being ethical is perceived to be as much about *why* you take a certain decision or course of action, as *what* you actually choose to do. This respondent and others suggest that it is the intention, or the motivation behind the activity which is of importance in defining whether behaviour is ethical. This is characteristic of virtue ethics. This 'virtue', or 'character' ethics as it is also known, is examined further in Chapter Six.

Despite this apparent difference in motivation, there seems to be a clear overlap in terms of the activity; they appear to be doing the same thing, but doing so for different reasons. One respondent indicated that he felt that the Ethical Hacker was influenced by the underground, or as he called it ‘unethical’ Hacker (see comment from Respondent 12 below) so that they have a certain level of influence over one another as well as shared activity that they engage in. It would appear that the Ethical Hacker responds to the actual known behaviour, and also to the expected behaviour of the Hacker, so that the cost benefit analysis may operate in the way that is described in game theory, whereby the ‘moves’ that are taken by each player are dependant upon what they expect the other player will do. For example consider the comment by one respondent that he “… think[s that] that the Ethical Hacker often has to adapt to a certain stance which has been brought about by an unethical Hacker” (Respondent 12).

This perception is also further supported by the comments made by respondent 16, who suggests that the Ethical Hacker is playing ‘catch-up’, which may be indicative that the Hacker has more influence over the Ethical Hacker than the other way round. He states that in his opinion “…the Hacker skill set is changing, and evolving all the time, and the Ethical Hacker is almost trying to keep up with that” (Respondent 16) .

This is of relevance as there would appear to be a link between offending, desistance, and level of skill. Previous research has indicated that “…Hackers with an average skill are prone to participate in malicious cyberactivities, on the other hand, highly skilled Hackers are more likely to engage in legitimate activities and disregard criminal ones” (Shim, Allodi, and Massacci, 2012: 1). This may be because they have more opportunities to use their skills in a legitimate way, so are less likely to offend through necessity. This is an example of choices being made that operate in a bounded way.

The skill level that an individual has presents them with different choices; this is optimisation under constraints as advocated within Criminological Rational Choice Theory (please see also Chapter Three for a discussion of the theory).

Within this research those that were the most highly skilled worked mainly in finance, and engaged in criminal actions. Those that identified themselves as having lower levels of skill worked within the public sector and did not admit to any criminality. This would appear to contradict the position with Hackers as identified by Shim, Allodi, and Massacci, (2012) whereby skill reduces the likelihood of offending. Heightened levels of skill make it less likely that the individual will be caught and prosecuted, therefore may mean that this risk is less significant in the cost benefit analysis of the skilled Ethical Hacker.

Many of the respondents, and particularly those with an underground background, differentiated between what it means to be an Ethical Hacker and to be a Hacker. One respondent further described the common confusion in the industry around the use of the terms Hacking, Ethical Hacking and penetration testing. He stated that:

> I think loads of people have the term confused. Many people actually interchange the term for penetration testing…Hacking is one thing and penetration testing is another thing. I think that Ethical Hacking is more of the mindset that the Hacker has…
>
> (Respondent 9)

The respondents to this study felt that there was some confusion within the field around the meanings associated with these terms, or else they otherwise did not see them as referring to the same set of activities as the response above indicates.

According to Mattford (2003) penetration testing is a key component of security. His definition states that:

> Penetration testing involves security personnel simulating or performing specific and controlled attacks to compromise or disrupt their own systems by exploiting documented vulnerabilities. Security personnel attempt to exploit vulnerabilities in the system from the attacker's viewpoint and are commonly referred to as white hat Hackers or Ethical Hackers
>
> (Mattford, 2003: 455).

The qualification as a Certified Ethical Hacker, or working as an Ethical Hacker or penetration tester, does not, it seems, necessarily mean that you see yourself as a Hacker, nor does it mean that you are necessarily accepted as being a 'Hacker' by those who have links with the wider Hacking community, even if engaging in penetration testing, or other typical activities associated with what academia has come to term Ethical Hacking. Dissatisfaction about this confusion was expressed by the respondents, one states that "I guess that that is what is the most disappointing part about the term Ethical Hacker, you can call me an Ethical Hacker, but, I am not a Hacker" (Respondent 2).

Being a 'pen tester' would appear to be something that you can learn in formal education, as respondent 11 indicates. He said that "….in order to become a pen tester I can easily come to the university here and get myself a degree" (Respondent 11). Other respondents concur with this view suggesting that "…any one can be a penetration tester. If you want to be a pen tester, you can just go to school and get a degree that says you're a pen tester..." (Respondent 2). Penetration testing is perceived to be a mundane job, where hacking is much more highly valued, "…if you are a pen tester you can sit round drinking coffee, but if you are a Hacker you are doing more important stuff, like Hacking" (Respondent 9) .

Being a 'pen tester' does not, it seems, make you a 'Hacker'.

> ….I've seen guys who are actually good at what they do as far as pen testing is concerned, they are much better than I am, but I just can not simply say that that guy is a good Hacker…..Once a guy graduates with an eth Hack – I mean an Ethical Hacking degree, immediately people think that he is a Hacker, but

> he's not, he might not be a Hacker… Some people graduate without knowing exactly what content is involved inside what they are doing technically, and ... erm, people do their homework for them, people do that every day, so there is no telling that the next guy to graduate from the Ethical Hacking degree is actually a Hacker
>
> (Respondent 9)

These comments would suggest that the concerns expressed by educators about teaching their Ethical Students how to hack are not as likely to realise themselves as they may expect. Hackers do not accept that people who have gone through courses of education are actually 'Hackers', being a Hacker is more about affiliations with the computer underground, and having underground knowledge than it is about being able to perform specific functions. The defining characteristic is not education, but rather it is membership of the wider hacking community, which also in itself does not necessarily mean that criminality is to be expected; many members of the computer underground only use their skills legally as is the case with FOSS hackers. Respondents who were educated but not affiliated to the underground were very unlikely to engage in criminality and they also suggested that they felt that this was the case within the field generally. This difference in community is expressed in terms of where individuals will go to access knowledge and support. One respondent commented that in his opinion the difference is that "…a Hacker is a guy who will go to RSC chat forums to get exploit code, yet a pen tester will go to security focus and web track, so it is actually quite different" (Respondent 2).

Some respondents did not differentiate between the Hacker and the penetration tester, often using the terms 'Hacker' and 'pen tester' interchangeably. This was the case for example, with respondent 4, who stated that "It is not that interesting to do a pen test; you just sit behind a desk like another bored person on 9-5 and just Hack away" (Respondent 4).

Being an Ethical Hacker would not appear to preclude one from also being an Underground Hacker. For some respondents it was not legality that defined an individual as being an Ethical Hacker, or as an Underground Hacker. It is notable that this view was common amongst those respondents who have described having underground histories or associates.

Being viewed as a Hacker would appear then to have its origins within having an underground socialisation and values; in the cases of the respondents who had been formally educated this underground socialisation was usually received before embarking upon their education in the field. Completion of a course of education or training in Ethical Hacking does not seem to be the differentiating factor; if it were the case that the course was the key differentiating factor, we would then expect to find more homogeneity of variance within the group of respondents and other Ethical Hackers who have formally studied Ethical Hacking. It is apparent that membership of the underground would seem to be a differentiating factor for the respondents in this study, but that it is certainly not the only factor which defines one as a Hacker – skills and mindset also being viewed as very important differentiating factors.

One respondent suggested that “There are people who are ethical when they Hack, and then there are people who are hired as Ethical Hackers” (Respondent 6); so Ethical Hacking as an activity and being ethical as a philosophical approach to behaviour are clearly not synonymous in the perceptions of all of the respondents. Their views on ethics, will be further explored in Chapter Six where we will explore normative and meta-ethical approaches in order to better understand how these impact upon their decisions and behaviours

5.5 Courses of Study for Ethical Hackers

There are now a steadily growing number of undergraduate and postgraduate courses in Ethical Hacking available at Higher Education establishments in the UK; this is in addition to the usually privately run 'Certified Ethical Hacker' (CEH) qualification. It is acknowledged that there is a benefit to educating people in Hacking skills because "…only very good programmers and professionals who have high probability of getting maximum pay-offs from legitimate activities are not prone to engage in criminal activities " (Shim, Allodi, and Massacci, 2012: 5). Persistence in offending among criminals has been found to be more common among those who do not have a positive turning point in their life (Laub and Sampson, 2003; Soothill et al, 2009) and it would appear from the responses to this study that there is the perception that a course of education can be a positive turning point within a Hacking career. While it may not completely remove the likelihood of criminal behaviour, it will certainly reduce the amount and the seriousness of the offending. McQuade (2006) concurs with this view. He suggests that education is necessary for making ethical hackers follow the professional standards of their industry. He states that:

> Through education and training people can better understand the rationale behind these rules, internalise potential harms and sanctions for non-compliance, and choose to abide by organisational and societal standards of behaviour on the basis of logic and reason for the common good of everyone
>
> (McQuade, 2006:144)

It is suggested that education and training help an individual to develop moral responsibility (Kohlberg, 1976), and therefore reduce malicious behaviour (Lipton, 2010; Broadhurst, 2006). This would appear to apply within this field as well as within understanding wider offending and desistence patterns.

Although the benefits of education are widely accepted, there has been some controversy about the use of the name 'Ethical Hacking' being used in describing courses of education which teach individuals how to use Hacking skills for security purposes. In response to the use of the term 'Ethical Hacking' within a course title for an undergraduate degree course at Northumbria University, the following was stated by the British Computer Society who did not agree with the way in which the term was being utilised as a marketing tool [emphasis in bold type is as it appears in the original source]:

> **Ethical Hacking** should **not** be considered to be an accepted professional industry term. If Penetration Testing is what is being taught, then that is how it should be labelled – rather than seeking to use marketing spin to gain traction and credibility within an industry that is seeking to improve its professional image. A teaching unit with the title "Ethical Hacking", whilst headline grabbing and engaging students, would not be a responsible way forward.
>
> (BCS, 2008)

The British Computer Society here indicated that they perceived the use of the term Ethical Hacking as being inaccurate, as misleading, and also as being potentially harmful to the reputation and to the credibility of the computer security industry.

One respondent who has completed an Ethical Hacking undergraduate degree course reinforces these concerns by questioning "…why not say it is a penetration testing course, because that is basically what you are doing, you are testing if you can penetrate a network" (Respondent 2). One of the education professionals who were interviewed for this research explains the reasons for this choice. He said that "…if we named a course 'Design of Security Counter Measures' we would get very few people involved because 16 and 17 year old kids just do not understand that" (Respondent 10).

The concern is that the use of the term Hacking might attract students with the intent to develop their abilities in order to Hack illegally, and to use the course as a way to increase their Hacking skills for unethical purposes. A current student of Ethical Hacking commented that within his student cohort:

> …you have got someone who could go either way, and at the minute they are called Ethical Hackers because of the course they are doing, but once the course finishes you can see them going off to become Hackers.
>
> (Respondent 12)

Although completing the course may reinforce moral and ethical awareness (Kohlberg, 1976) and therefore make offending behaviour less likely. A current student of Ethical Hacking stated that in his opinion "…people who have been through courses like this would have a stronger ethical perspective than those who have not" (Respondent 13).

He went on to describe the course he was engaged in. This was a mixture of practical sessions, law lectures and workshops relating to ethics, both philosophical and normative.

Some respondents had been unclear about the nature of the Ethical Hacking courses they attended at the outset. Respondent 22 describes his expectations and how they relate to the education that he received; he said that he had:

> …expected more education in Hacking and moving your way around a computer then spending the first six months on the course drilling the Computer Misuse Act into your head, and everything involving the legalities and that.
>
> (Respondent 22)

Respondents were asked about what they felt about the use of the term 'Ethical Hacking' as a course title and why they thought that people would want to call themselves Ethical Hackers rather than calling themselves security experts or penetration testers, or secure systems designers. This was in view of the fact that it was becoming apparent that many of them did not see the course as able to ‘make’ someone into a Hacker. It would appear that the use of ‘Ethical Hacker’ as a title is about creating and increasing individual employability in a growing sector and marketing courses in an appealing and accessible way.

Some of the respondents discussed the use of the term suggesting that they agreed that it may be useful for marketing, or as an informative measure, so that potential students and employers with limited industry knowledge would understand what the aims of the courses were. One respondent describes this situation saying that “…if you have a course in penetration testing at a University, but you call it penetration testing, people do not know what it is…” (Respondent 3).

It would appear that for the individuals involved, having the title of ‘Ethical Hacker’ is perceived to increase their level of employability within the sector:

> …once you say you are an Ethical Hacker…you will get hired because right now, in the industry people really need that, they really, really need that, I mean, right now, I am working for this company and we see loads of work coming in because, erm, people are getting Hacked, people are getting breached and people want to get their networks secured from that so they look for an Ethical Hacker or penetration tester to come and check if their network is actually secure.
>
> (Respondent 9)

Despite this there are concerns within academia which mean that there seems to be a reluctance among professionals to offer courses in Ethical Hacking, and where they offered, there are concerns about using the term ‘Ethical Hacking’ within the titles. Respondent 16 describes this situation saying that:

> Academically, there are not that many places offering it, and I think that people are still a bit nervous. They do not quite get what it means; they see Hacking and think whoa, too dangerous, too scary…I’ll try to push the notion of Ethical

> Hacking as a respectable discipline. I think there is still a lot of work to be done on that to be honest.
>
> (Respondent 16)

He also notes that Ethical Hacking courses can attract the 'wrong sort' of student,

> We are very aware that the skill sets that are being developed could be used for you know, underground activities….I put in place an additional student behaviour form that they had to sign and you know, say, that you realise you can kind of misuse these skills, and if there is any evidence of that at all you are on the streets…I was always petrified ...that some student had developed Hacking skills and I would be the face in [names a local newspaper] that they were blaming.
>
> (Respondent 16)

Respondent 16 is here describing a cost that he has added the cost-benefit analysis of his students in deciding whether they will offend using the skills that he has taught them; they will be removed from the course if they are caught. The student will, according the bounded rational decision making model, weigh up the potential likelihood of being caught and prosecuted and will then decide whether or not to engage in illegal activity based upon this calculation (Clarke and Cornish, 1985; Cornish and Clarke, 1986; Cornish and Clarke, 2008). This would suggest that the possibility of losing the opportunity for education and for future employment could act as a deterrent. This is clearly the hope of this educational professional in introducing this sanction.

This is accompanied by the hope that the personal intentions and motivations of a black hat Hacker can be turned around by being involved in a course of formal study.

> You get one or two people coming in who... you know… they are potential black hat Hackers. The challenge is to turn them round, but others come in and they sort of realise the situation and they do want to do that security design. They do realise that it is a positive thing rather than a negative thing…I mean we batter into the kids about professionalism, and a sense of ethics, and err so maybe that is part of it.
>
> (Respondent 16)

Respondents who were previously, or are currently Ethical Hacking students described their reasons for choosing to study the course. None mentioned that they were motivated by the desire to learn about ethical approaches, rather they discussed employability, and they discussed skills.

> A lot of people on the course realise that it could lead to a very well paid position so if you have got background knowledge or a back ground interest it is a nice way to pursue something which you are interested in and security like for the future
>
> (Respondent 8)

This would indicate that part of the motivation for Ethical Hacking is financial; financial security and job security often being discussed together as being motivational factors. Respondent 12 is illustrative of this point; he stated that "…I suppose it is about money for me. I know that when I come out of this I can settle into a well paid job" (Respondent 12).

Many Ethical Hackers indicated within their interviews that they chose to be Ethical Hackers because of the financial rewards within a growing industry. Financial gain is not apparent in the extant typologies of Hackers as a motivational factor (please see chapter 2), so this is significant in that the motivations for Ethical hacking are different to those of traditional forms of Hacking. Employability seems to be a very important motivational factor in choosing to engage in courses of study and to work within the sector and will therefore be discussed further in the next section.

5.6 Employability in the Sector

Respondents all acknowledge that the sector is growing rapidly and that there is therefore an increasingly significant market for the skills of an Ethical Hacker.

According to one respondent “…it is becoming a big business area.” (Respondent 4). The nature of the industry, and also societies increasing reliance on information communication technology within wider society mean that Ethical Hackers feel that there is a future career that they can pursue on offer, as the following comments show:

> I think there will always be a need for people like me… So much of what we do today is related to computers and networks…So, if that is the case there will always be people who are trying to abuse these, and that is where I come in (laughs)
>
> (Respondent 7)

This would indicate that there is the perception among respondents that as well as financial gain, the sector offers job security and also the possibility for career development. An example of this comes from respondent 2 who said he “think[s] it is a really special area, and it is growing, and [he does] not see [him]self leaving it for a long time, because it is growing, and people need it.”

5.7 Roles, Responsibilities and Employers

As well as the expectation that they will work within the law themselves, Ethical Hackers are expected to have the intention to ensure that others also operate within the law. The role of the Ethical Hacker is described as being preventative. “Ethical Hackers try to stop the crime from happening in the first place” (Respondent 10). Respondent 16 describes the nature of the industry:

> I see Ethical Hacking as a tool for the safe design of computer systems, so people that are involved in security aspects of the design of computer systems.
>
> (Respondent 16)

As well as new product design, Ethical Hacking could also entail finding security problems that pre-exist in systems that have been designed by other individuals.

The Ethical Hacker is taught to how to design systems that are secure, but also to find flaws in extant systems and to fix them. The focus is to be proactive in approach rather than reactive. An educator defined the role of the Ethical Hacker by saying that he " see[s] the Ethical Hacking work as a case of finding problems with security, and being proactive in that rather than reactive" (Respondent 16).

Respondent one was critical of this approach, he felt that software solutions were a problematic option stating that "…you can only have so much defence before security outweighs operability" (Respondent 1); he suggested that this is because security software tends to be very costly to design and to implement and it will also slow the operation of systems.

Educational professionals, students and programmers tended to take this pro-active view to the activities that they saw as defining the field. Ethical Hackers are therefore employed in prevention of rather than detection of crime, according to this perspective. One Ethical Hacker stated that:

> The Ethical Hacker is doing it to find vulnerabilities and weaknesses in a system, or a computer network, or whatever it might be, and to then tell the person that they are working for that are these weaknesses, and here are some security designs to plug those weaknesses and get rid of those vulnerabilities and make it a better safer system at the end of the day.
>
> (Respondent 8)

Those individuals who have entered Ethical Hacking from policing, law or security backgrounds tended to take a more reactive approach within their roles. One respondent who utilised Ethical Hacking techniques within his role as a police officer described this reactive approach. He stated that his "…purpose of it is to catch those people who do those sorts of things for the malware aspect of it, the stealing of data, the manipulation of data, the general pissing people off …" (Respondent 14).

The descriptions from the respondents about what they do within their work roles and who the clients and employers that they do it for were very varied. One commented that initially when he entered the field he "...didn't think it was going to be this diverse" (Respondent 11), this diversity is also noted by Coffin (2003) who states that "…what goes into Ethical Hacking depends on the range of services required, the size of the client and how much that client is willing to pay (ibid: 2003: 1). The diversity in the job is reflected in the diversity of employers and of roles and responsibilities within the work. "There are all sorts of different sets of employers that would employ an Ethical Hacker, whether it is a security system or an IT security system, or whether it is a government agency or a private forensics firm" (Respondent 10).

It would appear that within this diverse range of organisations and individuals seeking the service, that there are two main types of employers who will hire Ethical Hackers. Firstly there are those who want the particular problem to be rectified on their behalf, and then there are those who want to actually understand the nature of the problem and to be able to prevent it from happening again. In describing his usual employers one respondent indicated that in his opinion:

> …there's two types of guys – there's the guy, the finance guy, who'll come and say 'hey, can you check if my network is secure, because there is an audit that is about to take place' so we just check if its secure, and if it is say 'yeah, it's secure' and if it is not say 'it's not secure', and then there is the IT guy who really wants to know how to fix it.
>
> (Respondent 9)

There is also a clear distinction between private and public sector work, with private sector work seemingly being more lucrative, and more consistent.

> …. In the public sector who knows if a guy is going to steal or who knows if a guy is going to be a paedophile tomorrow, because there are loads of those cases coming in, but who knows if a case like that is going to come in? If for example a company wants a bank to a status acquiring bank wants a merchant

> number you will need to be PCI compliant, you need to call in a computer security expert, you need to call in a penetration tester each and every year to test the network for you.
>
> (Respondent 9)

Employers seem to be quite varied within both the public and the private sector. It would appear that this can be any kind of organisation with data that has a value to them, and that in particular financial organisations are very significant employers within the sector. Data that needs to be protected can range from sensitive personal data to financial data. Respondent 9 elaborates on the range of clients that his employer provides services for:

> …we have banks, merchants themselves can come in, like, erm, huge multi-national corporations have actually come in, and educational institutions come in, erm, anybody who has a network that they value, comes in and just says 'hey, can you just check that my network is secure'
>
> (Respondent 9)

It would appear from the comments made by respondents that a large proportion of their job role is administrative, with a lot of the Ethical Hackers time engaged in non-Hacking activities. This may act as a disincentive to become involved for those Hackers who hack obsessively or compulsively. One respondent indicated that despite common public misconceptions "…breaking into systems is only 20-30% of your job, the rest of it is writing up reports and risk assessing" (Respondent 18).

When talking about what their roles entailed, the topic of penetration testing came up frequently. As previously discussed, respondents do not agree about whether penetration testing and Ethical Hacking are the same or not. Some respondents saw these as being one and the same, where others perceived penetration testing to be only one part of what an Ethical Hacker does in their usual work. One respondent clearly described his perception that penetration test is only part of the job, and therefore could not be considered to be fully synonymous with it stating that "…as far as I am concerned there is two main sections, penetration testing and infrastructure testing" (Respondent 19). This view is common among the respondents, Respondent number 7 providing another example: "Penetration tests are only one part of what I do, I also have to do some forensic stuff for a contract that we have" (Respondent 7).

Some of the respondents use the term interchangeably, while others describe one as being pro-active, and the other as being reactive.

> I do not see those as being the same thing at all, as I say, two sides of a similar coin, but opposite sides of that coin. Computer forensics, whilst it can be proactive, and by seeing that there are forensic principles in place it might act as a deterrent, the forensic side of things is very much looking at a cyber-trail and trying to find evidence which is then going to go to court. The Ethical Hacking side of things is just a completely different pathway. It might be that be that a person has both sets of skills, but they are divergent paths. You might use some Ethical Hacking skills in a forensic investigation, you might use some forensic skills in an Ethical Hacking approach but I see the Ethical Hacking work as a case of finding problems with security, and being proactive in that rather than reactive as computer forensics is very much reactive, and once a crime has happened you throw in the forensic skills, Ethical Hackers try to stop the crime from happening in the first place.
>
> (Respondent 16)

There would appear to be a clear distinction, in the view of this respondent, between computer forensics and Ethical Hacking.

5.8 Employability of Ex-criminals

There is much debate within the industry, and among the responses of those this interviewed for this study about whether it is acceptable or useful to employ as Ethical Hackers those with criminal backgrounds. Furnell (2002: 234) suggests that employing ex-criminals will be beneficial course of action for employers because "…a system will be subject to a more realistic penetration attack, conducted by exactly the sort of person who might otherwise be trying to break in". Whilst it seems that it may be acceptable to have gained knowledge through being part of the underground community, and having previously been involved in criminality, the line seems to be drawn at having a criminal record. This would preclude the Hacker who has decided to cross the line from being an Underground Hacker to being an Ethical Hacker from being able to gain employment. (The development of the legal framework and responses to it were outlined in Chapter Two, respondents views on the law will be discussed at length in Chapter Six; this section will specifically focus upon the perceived employability of ex-criminals.) One respondent said that he felt that it was tolerable for an Ethical Hacker to have a criminal background, but only if they did not have a criminal record; the criminal conviction, rather than a known criminal background precluding the individual from employment. He said that "…you can tell anecdotes, but if you had a record then you wouldn't get the job" (Respondent 8). The criminal record, rather than actual criminality would appear to be the defining factor.

The educational professionals interviewed did suggest that some of the activities that they had engaged with in the past, before the Computer Misuse Act 1990 criminalized those activities, would now be illegal; the students and ex-students interviewed also suggested that their lecturers were happy to share pre-criminalization examples of activities that they had engaged in that would now be classified as being illegal computer misuse.

Those respondents who had underground affiliations, and/or a criminal background were disapproving of the hiring of previous criminal Hackers as they indicated that they felt that these individuals would be difficult to trust, and that any suggestion of illegal activity could potentially put the reputation of the business at risk. In support of this, Furnell (2002) questions whether the hacker is trustworthy, whether they may leave back-doors into systems for themselves (or others) to use at a later time, and also suggests that if they remain affiliated to the underground community, completely securing a system would be in contravention of the Hackers Ethic (Levy, 1984).

Despite suggesting that there are issues in employing those with a criminal background, respondent 9 suggests that if he was to be caught engaging in criminal behaviour he would still wish to be employed, although he would not expect this to be the case:

> Obviously if I get caught one day doing something I would want a job, but I mean, I wouldn't blame the guy who does not hire me because I have a criminal record.
>
> (Respondent 9)

Respondent 13 identifies some of the questions that employing ex-criminals raises for the employer:

> Are they going to stay on the straight and narrow or are they going to veer off if they see something in the business that they know they can take advantage of and remain anonymous whilst they are doing it? It is kind of a risk.
>
> (Respondent 13)

There are clearly issues around trust, as indicated by the following comment from respondent 2, who himself admitted to engaging in acts that are illegal, but which he saw as being harmless:

> I think they are going to have problems with that [hiring ex-criminals]…who is going to say that those guys won't steal from them.
>
> (Respondent 2)

Some respondents suggested that the concern should be for the customers who buy the service rather than the employers. Employers have a choice regarding which individuals they choose to take into their employ, customers however are acting on assurances that they are will be having their sensitive data, and their systems handled by a person who can be trusted.

> It is really not fair on the type of customers that you would be dealing with…you are telling them that you will sign a non-disclosure agreement, and say that all of your pen testers are properly qualified, and they are guaranteed not to steal and information…it is just not fair.
>
> (Respondent 23)

There are also concerns expressed about the impact for other employees, as well as the business. These other employees could be perfectly legitimate, yet any negative impact on the business will also impact upon their employment, and their professional reputations, as is shown in the following comment about criminal employees:

> If he is yours and he is caught, the company goes down; you can not take the risk because if he goes down, everybody else is going with him. Everybody could lose their job because of him.
>
> (Respondent 23)

Others respondents were more positive, suggesting that actually a criminal or underground background could potentially be an advantage to the individual and to the employer. The Underground Hacker is perceived to have the requisite skills, knowledge and abilities to be employed as an effective Ethical Hacker. Respondent number 8 said that he "…think[s] that it is quite a good idea to be honest [because] you know that the person you are taking on will have the skills set" (Respondent 8).

Furnell (2002) suggests the following benefits of employing individuals who retain their affiliations with the wider hacking community:

> …as a member of the hacking community, the hacker may have a number of advantages when compared to some security professionals, including familiarity with the latest hacks, and the ability to gain access to information from other hacker contacts.

(Furnell, 2002: 234)

He goes on to say that

> ...the hacker's personality and motivation (i.e. driven by the challenge and enjoyment of beating the system) may lend itself better to the task of uncovering further vulnerabilities than a standard security consultant, who may simply be working through a checklist of known potential holes
>
> (Furnell, 2002: 234)

Furnell (2002) clearly distinguishes between two different types of Ethical Hacker, firstly there is the 'hacker for hire' who tests systems, finds holes in their security and then approaches a company in search of employment, and then there is the Ethical Hacker who is directly employed and commissioned by the company. He suggests that it is preferable if the company approaches the Hacker, rather than the other way round. Hackers who approach companies seeking employment are, in his opinion, less likely to be trustworthy, he raises the question about what these individuals would do if not employed, given that they have an awareness of security issues, and also raises concerns about the precedent that this sets, which could effectively encourage other individuals to repeat the behaviour and to hold the company to ransom.

Some respondents could see the range of benefits for the employer, but they suggested that they did not want to have those Ethical Hackers who have a known criminal past as a work colleague:

> I can see why people would want to do that, I am not sure I would want to work next to a criminal, but I can see why an employer would hire one. I mean, what if I am working with someone, and then they are doing bad things? I can get the blame and then that is both of our careers over. No, it is a bad idea.
>
> (Respondent 7)
>
> They might be good at their job, but why would you trust a person like that? Hiring criminals is not fair on us who have gone by a legitimate route. I wouldn't want my employer to hire criminals, but I guess I can see why he would…

(Respondent 23)

Those who were positive about employing those with illicit skills were more likely to have no criminal history, and/ or a background in policing, law or security. Some went further, suggesting that they felt that having criminal knowledge was *necessary* in order to ensure that the person had the correct knowledge to carry out their role efficiently.

> 90% of the people I know who are Ethical Hackers were ex…wrong side of the tracks. There is nobody better to keep somebody out, than somebody who knows the tricks and the lifestyle and how the other side lives, because you know what they are about to try, you know what to defend against.

(Respondent 1)

It was also suggested however that even with an underground background, the benefits would diminish over time as the individual's underground affiliations and illicit knowledge would diminish over time:

> …once those guys are recruited, and once they are working for the government or whatever, well then there is that little element that well, you are out of touch with what is going on underground.

(Respondent 2)

In the early days of the industry it was common to see media stories of convicted Hackers becoming co-opted into large security or financial organisations. It would appear from the responses to this study that this trend is perceived to be waning.

> People that were breaching systems, particularly of financial institutions, the banking institutions were employed, rather than, say the banks, saying you have breached our system, you know, come and fix it. That trend seems to have stopped. I do not know if that is because of the Ethical Hacking courses are contributing to that.

(Respondent 16)

While respondent 16 suggested that this phenomenon could possibly be in part attributable to the growth of Ethical Hacking courses, which provide a skilled professional as an alternative to the criminal employee, it may also be the case that businesses do not wish to take unnecessary risks with their reputations as outlined above, nor do they wish to publicly encourage Hackers to breach their systems as a means of securing employment.

Respondent 2 suggests that employing ex criminals is neither effective (as they are not very skilled, having been caught) nor is it necessary (as there are better alternatives available), and therefore it cannot be considered to be a rational choice for the employer to make in terms of the outcome; it would be more rational for then to take into their employ an educated professional. He states that:

> If you want someone who is good at their job, he ain't getting caught. You have got a criminal, and not a very good one at that. Employ the person that is better, if you can find him. We have enough education and academic people in the field to get away from that. We do not need them any more. ..He is criminal. The trust is gone. You have broke the law. You did it, you got caught.
>
> (Respondent 2)

As Kevin Mitnick states, whether to employ someone with illicitly gained skills is a choice to be made by individual employers, who must themselves make a cost benefit evaluation of the impact of employing an ex-criminal:

> This question is really a question of balance. Does the prospective employee (former Hacker) bring enough knowledge, experience, or skills that outweighs the risks associated with hiring that person? You have to closely examine the background, values, beliefs, goals, and attitude, to gauge the risk to the business. In some cases, the person can be hired to perform a service that is a low risk or even risk free. I firmly believe that once a person has paid their debt to society for past transgressions, that individual should be free to pursue legitimate employment opportunities that benefit society.
>
> (Mitnick, 2003)

Again though, this reasoning is bounded (Simon, 1957); it relies on the employer knowing about the criminality of an applicant. All they can know for sure is whether the applicant has previously been prosecuted, and not whether they have actually engaged in criminal behaviour.

5.9 Home and Work

Many of the Hackers who responded to the study, with the exception of police officers, security professionals, lawyers and educational professionals, reported that they would act as Ethical Hackers during their work day, but that they were actively engaged as part of the computer underground in their own time, often using skills, knowledge, or information that they had gained at work. Even though completely adhering to the law in their employment, it was not uncommon to find Ethical Hackers who were engaging in illegal activity in their own time. In describing the field generally respondent 6 stated that: “A lot of the people that they hire are ex Hackers, or current Hackers who just happen to have a white hat on…” (Respondent 6).

Respondent 15 concurred with this opinion when discussing criminality, he states that:

> You find that the Hackers who get caught are working somewhere else as well, they are working for companies, or they are security experts or whatever and they did something dumb and they got caught.
>
> (Respondent 15)

They often did not overtly state that they were involved in illegal activity, but would imply that they could be if they wanted to as they had the skills and the access that would enable this. It was often the case that when the respondents were not making use of resources that they had access to through their work, they did enjoy the knowledge that they could if they wanted to, gaining a sense of power from this. This supports Jordan’s (1999, 2009) conception of a techno-elite, who hold power through the knowledge that they have regarding technology.

> ...if you are doing an external pen test and you know that you have got access to such and such a number of computers or servers, say ten computers or ten servers, and if you know that you control them, you know you need them for something else, it is something else to give them up even if you know that you have to…
>
> (Respondent 9)

Jordan and Taylor (1998) suggested that Hackers in general enjoyed the feeling of having power over a system. It would appear that a number of the Ethical Hackers have this in common with the Hackers studied by Jordan and Taylor if we consider the following comments as examples:

> …who is to say that I didn't actually put a shell script into it or something like that to actually get myself a back door…?
>
> (Respondent 2)

> …even if everyone else is actually covered from it, I still have a back end to get into it…"
>
> (Respondent 15)

> …even if you go to work and you're doing a pen test, and you go back home and you're Hacking as well…
>
> (Respondent 11)

This regular and frequent switching from legitimate activities to the illegitimate activities may be because the individuals who are involved are seeking a new personal challenge as they no longer find any challenge in either Underground Hacking or in Ethical Hacking, so switch from one to other as desired to prevent stagnation and boredom. One respondent in particular felt that there was no challenge in Ethical Hacking because there was no risk attached, and no law breaking involved:

> If these guys have signed you off you know that nothing is going to happen to you. Totally nothing is going to happen to you. They expect you tell the truth because you are the expert, there is 100% no challenge to what you do.
>
> (Respondent 4)

For those respondents who continued to engage in criminal behaviours, despite working as Ethical Hackers, it may be worth considering that the level of risk can variously be a cost or a benefit within a cost benefit analysis. While the possibility of being prosecuted would usually, for most of us, be considered a negative within a rational cost-benefit calculation, criminal Hackers have been found to be "…more prone to engage in potentially risky behaviours than members of the broader population" (Bachmann, 2010: 652). This may indicate that the level of risk increases the sense of thrill, and risk is therefore perceived as being a positive within the rational calculation, increasing the level of challenge.

Those who had their own means of securing access preferred to keep Hacking for work and Hacking for leisure as completely separate activities. They would only use knowledge and access that they had gained at work if they had no other means of securing access

> …if its work related, I try not to get to a stage where I say I think that I might use this companies server for this, or I think I might use these peoples computer for this, I try not to get to that point. I try to…give them everything; I try to just get rid of everything. If I ever have an exploit that I want to run I try to just look for my own server to do it on, it is quite easy to sniff out the internet for a server. It is really, really easy so I try to have line between the type of stuff that I do, you know the exploits that I find when I am at work and the type of stuff that I do when I am just doing my own stuff at home because its better that way.
>
> (Respondent 9)

The line between being a Hacker and being an Ethical Hacker seems to be a very fine one, many individuals being more accurately described as 'grey hat' Hackers than as 'black' or 'white' (see Graves, (2007) for definitions of black, white and grey hat hacking), and many other individuals completely changing their ‘hats’ depending on who they were Hacking for and where and when they were doing it. One respondent states that he “...always dabbled on the side in [his] own personal time…” (Respondent 18).

Respondent 2 describes his perception:

> I think that if you take a look at it using a normal distribution curve, the shade of grey is in the middle, you know, the whole 90% in the middle, that is how grey it is. There is so much ambiguity; it is a very, very fine line. You can do it [cross the line from Ethical Hacking into illegal forms of Hacking] just like that, it is just so easy.
>
> (Respondent 2)

Ethical Hackers who were engaging in illegal activity or sharing illicit knowledge were generally those with underground backgrounds or connections. This meant that they had access to illicit knowledge and to Hacking tools that may not be as easily accessible without engagement with the underground community.

> …I have the exploit code because I know people right now, I know guys and if I get an exploit we can share it…
>
> (Respondent 11)

> I know who to go to for the next exploit, but they are not giving me anything without getting something back. I can get new stuff, but I have got to find new stuff too, and clever stuff, or they won’t give me nothing. Sometimes you just end up going from one to the other passing each others stuff around
>
> (Respondent 2)

> At least a third if not a half of my week was spent on discussing with people, various underground message boards and things like that and just keeping up to date with the latest exploits that are coming out…
>
> (Respondent 1)

Those with security, policing, or law backgrounds did not engage with the computer underground, or at least did not admit that they did.

Many respondents felt that an effective Ethical Hacker, or to be a good Underground Hacker, an individual had to have some of these social connections with the computer underground, and that it was also necessary to nurture these relationships, “... a Hacker is a guy that has friends underground...” (Respondent 2).

The lack of these connections would explain why in some cases, Ethical Hackers are one step behind the development of new criminal activities because “…you have got to keep your nose a little bit dirty just to keep up with what is going on…” (Respondent 1)

Whether we see Ethical Hackers as actually being ‘ethical’ clearly depends on which ethical approach we take (please see Chapter Six for a full discussion of these approaches in relation to the decisions and behaviour of the respondents to this research); it also appears that they are not consistent in their behaviour and the decisions that they make. They can be engaged in acts that are legal by day and are criminal by night, as one said of his activities at work “…when I get home, I can do this again…” (Respondent 19).

It is worthy of note that although the activity may be identical, it is criminalized in one context and celebrated in another. In fact it may just be the distinction of where and when the activity is carried out which makes it legal or illegal, and therefore normatively perceived as being either ethical or unethical, right or wrong. This may make it less likely that Ethical Hackers see their own illicit behaviour as being ‘wrong’ as there is no clear distinction between what they actually do in terms of the activity, this will make it easier for them to rationalise sliding from one type of activity to the other. This would support Leibrich’s (2003) conception that going straight is often more accurately described as ‘curved’ in that the offender is neither fully ‘straight’ nor fully ‘crooked’. Respondent 2 disagrees with Leibrich, he said that in his opinion “…you just can not play for both sides, at least at the same time; you can not be a good guy and be a bad guy all at the same time (Respondent 2).

One respondent attempts to rationalise his own involvement in underground activity and collecting illicit knowledge by suggesting that it may actually be to the benefit of his clients and therefore is justifiable. He states that:

> You are using the same skills, the same knowledge, you use the same tools. If I get something else underground, and I go to work tomorrow, and then there’s a really big client with the same application, what better way to please him than to use the exploit code that I got underground?
>
> (Respondent 9)

Ethical Hackers can also alter their career path from being Underground Hackers to being Ethical Hackers at the mid point in their Hacking careers. This phenomenon and the reasons for it will be explored in the following section.

5.10 Moving from Underground Hacking to Ethical Hacking

There is some anecdotal evidence that affiliation with the computer underground is something which changes over time (as discussed in Chapter Three) with Hackers choosing to desist from criminal activity as they age. This is well documented in relation to other criminality and deviance (Soothill, et al, 2009); it could be that this is due to changes in lifestyle (ibid), or simply a more mature approach to moral decision making (Kohlberg, 1976).

Respondent 16 thought that the decision to desist from criminality and to engage in legitimate employment using their hacking skills was a rational choice that Hackers made, based on an evaluation of the level of risk.

> Well it seems to be that Hacking is a young persons skill and they are all locked away in their bedrooms, by the time they get to about 25 or 30 they realise that, oh, there is a life out there, or they get caught and they realise the risks that they are taking and they come to be more risk averse as they get older.
>
> (Respondent 16)

Other respondents indicated that they had changed their behaviour as they aged:

> I look at the kind of attacks I was doing when I was sixteen, and that is exactly the type of person that I am trying to keep out now.
>
> (Respondent 6)

> That is [DDoS attack] not something I would ever do now
>
> (Respondent 15)

> I found myself not just protecting my site, but seeking a little bit of revenge for things which may have been done to our forum. That was a good ten years ago and is something that I wouldn't dream of doing now. That may be because of getting old and perhaps the course has something to do with it.
>
> (Respondent 12)

It was suggested that desistance with age was linked to reduced levels of status being attached to Hacking for older people whereby the perceived rewards of the activity are reduced. He also expressed the need to be socially desirable to wider society, and to make a living in a stable and legitimate way as rewards of acting legally:

> Obviously, if you are 18, and you are Hacking, then you are so cool, to all your friends, once you get a bit more old and you get a bit more maturity, there is actually not that much to it. I can do it, but who am I trying to look cool to, but I need something a bit more stable. I need something that shows who I am, I need to legally erm, I need to do what I do in a more legal manner, and make a living properly just like every other person is doing.
>
> (Respondent 20)

Respondents who are in stable employment indicate that this is a choice, and that alternatives have been considered:

> I have thought about going to the dark side.
>
> (Respondent 10)

According to Leibrich (2003) offenders will weigh up the worth or personal value of offending behaviour, and the relative benefits and limitations, including the emotional inputs and outcomes, and so the decision to desist is understood to be related to reduced benefits or increases in perceived costs. Some Ethical Hackers described this situation, for respondent 15 for example there had come to be less enjoyment in illegal Hacking, and no risk involved in Ethical Hacking, as he describes:

> There is only so much that you can do, there is only so much fun that you can have, the time is coming when the fun will run out, and you just have to move with the times. If it means going to a security company to do it legally then so be it. You'll just be sitting behind a desk like everybody else, you know? With a smile on your face knowing that no-one is chasing you.
>
> (Respondent 15)

Respondent 9, in agreement with the comments from respondent 15, identifies the level of risk as being a significant motivating factor which he suggests causes people with a background in Hacking to choose to move over to Ethical Hacking. He says that in his opinion Ethical Hackers can be defined as:

> …people who have had experience of Hacking previously and do not want to risk it too far illegally and they want to apply what they have done legally and what can be done openly I think that is quite a big drive for some people.
>
> (Respondent 9)

Respondent 20 suggested that as the Hacker ages, there is a reduced need to 'look cool', and describes the possibility of becoming disinterested in illegal Hacking:

> You can get into a thousand computers, or you can do a DDoS on the Whitehouse, and you can look so cool. You do grow out of that. Somehow, maybe it just might grow boring. I haven't come to that point, but it might grow boring.

(Respondent 20)

It may simply be that those individuals who are involved in Ethical Hacking have chosen this path because it provides them with employment that they find enjoyable; they are able to be employed in an activity that they would choose to engage in even if it were not part of their work, as one said, “It is a lot better to go and work somewhere where I actually like doing this, this is a good hobby” (Respondent 17).

Some indicated that although they agreed that Ethical Hacking was engaged in because it was enjoyable, they needed to find a way to utilise their skills legitimately. They suggested that this employment also may enhance their ability to act efficiently in their criminal behaviour by providing skills, resources and opportunities:

> You need to find something that you can actually do as a career, and what better choice than something that you do in your spare time? Or something that you would use to gain more skill to go and steal some more credit cards?
>
> (Respondent 9)

It is evident that after some time the perceived challenge in Hacking illegally is reduced. As previously discussed challenge is identified as being an important motivational factor. Once the challenge is reduced, the individual is therefore left with the skills and the knowledge to hack, but not the drive to do so.

> …after quite a while I mean the challenge goes [pause] once you have proven it to yourself the challenge is absolutely gone [pause] erm [pause] because there is nothing more to it.
>
> (Respondent 19)

The pauses in this comment may indicate that the respondent struggled with explaining why he sensed that the level of challenge was reduced. Other comments were also indicative of a reduced sense of challenge:

> You start Hacking into networks, you break this one, you break that one, you break this one, and you break that one. You know your neighbours key, you have it and then what? But you've got your own internet and they have got their own internet so then what? You know that even if you get into their computer it is boring as hell.
>
> (Respondent 15)

The rewards of illicit Hacking activity are reduced over time, and with ageing, so as a consequence the individuals that are involved will seek to find alternative rewards, however they still wish to make use of their existing skills and their knowledge. As well as new forms of challenge as previously identified, the benefits sought can come in the form of financial rewards, job security and in prospects for career progression.

Responsibilities come with ageing, and these can impact upon the choices that are made about behaviour as the following comment indicates:

> You can not make a lot of money from showing off to your mates how to shut down a PC and it comes a point in your life when you have to make money to pay the bills.
>
> (Respondent 1)

Some of the respondents suggested that they felt that as they grew older they increasingly needed the security of knowing that they had a regular income, as they felt that earning an income from illegal activity is not as easy or as secure as the general public might expect; that "…underground it is really hard to make a living, and you have to make a living" (Respondent 9). This is described as being due to the amount of illegal activity online, and the proliferation of, and easy access to exploits underground.

> It is really, really, really hard to make money, or to live, Hacking into peoples networks, so you need something, right now I could be getting credit cards or whatever, but underground, credit cards are quite cheap, even if I have loads of credit cards, credit cards are quite cheap, I can get a credit card, for like £2.50 because there are so many tools that you can use right now to get them you don't really need that really clever Hacker.

(Respondent 9)

It would therefore appear that many ‘cross the line’ from Underground Hacking to Ethical hacking because they become bored, because they need a new challenge and because they need to secure an income. They also see little challenge in using many of the exploits that can be accessed online, which they perceive to be an activity requiring of low levels of skill.

5.11 Social Organisation of Ethical Hackers

In Chapter Two we saw that the Hacking Underground is a community which offers a network of support for its members, and is hierarchically structured.

Ethical Hackers do seem to have some level of social interaction, and even community, but cannot be understood through the power hierarchies that are apparent in the Hacking community (Jordan, 1999; 2009) or as a force for social change. Referring to previous research on the Hacking community, one of the educational professionals interviewed for this research said that he felt that there was not the same hierarchical structure in Ethical Hacking social organisation, or that if there was, it was not apparent to him. He states that:

> “There has been a lot more work on why certain types of Hackers work alone and why some group together, and why there is a kind of ‘pecking order’ of 'Hackerness'. I do not see that same thing in Ethical Hacking”

(Respondent 16)

When specifically asked whether he felt there was the same sort of community (as is described by Jordan, (2009) in relation to the Underground Hacking community), this respondent indicated that he felt that “..there may well be, but [he is] just not party to it."(Respondent 16) He said that he had "…steered clear of Ethical Hacking groups, [and that he] really [didn't] know why" (Respondent 16). He did not engage with the networks that existed, and was unsure of how they were socially organised, but was aware that there were Ethical Hacking groups.

A respondent with a policing background described computing and its related community and culture in terms of its utility and not as being something that he engaged with as a leisure activity. He states that he does not "…frequent any of that computer culture," because "…it is just a tool for me at work. I go home and I use it as a tool." (Respondent 21)

Other respondents clearly saw a network which offers collegiality and support, and is not hierarchical in the same way as that found in the underground community:

> …all the lads just help each other out you know? Its not like online Hackers, they wouldn't give you nowt, unless you had something for them. At the end of the day it just means more work for me if I am on a job with someone and they haven't got a clue what they are doing.
>
> (Respondent 1)

Respondent 9 supports this perspective. He gave a very clear description of training and supporting a new colleague, which would support the idea of community, and of a network of support, but would not support the idea that there are similar power hierarchies as have been described as operating within the Hacker Underground (Jordan, 2009). He said that it was

> ..totally the opposite. You get some guy, he is a pen tester, he is in security, he is new, you try by all means to get him up to speed, because that is what he is here for, and you are going to share all of the information as quickly as you can.
>
> (Respondent 9)

When asked about how this compares to the Hacking community, he goes on to say that in his opinion:

> It is directly the opposite, you have to try and teach a guy who does not know. If you are a pen tester or if you are security, you have to try and teach your colleagues or whoever, you just have to try and teach them to get them up to speed. At the end of the day you both Hack, you can not be going out on a job on a case onsite with a guy who does not know how to Hack, because at the end of the day you will be doing all the work. And number two, it is actually helpful, he actually gains quite a lot, and I think it is totally the opposite if you go to Hacker forums. If you do not have anything then you do not get anything. It is just that way, or at least I have seen it to be that way…
>
> (Respondent 9)

Notably, respondent 9 was one of the ten respondents who described engaging with both the Underground Hacking community and the Ethical Hacking community. As a member of both, he is appropriately situated to describe the differences. He continues as follows, describing how and why he would support a new colleague:

> You are going to sit next to him and Hack with him until he learns; I mean that is how I learnt. If I could not get into a database I would sit right next to another guy, even if he was typing at ten thousand miles an hour and I would see how he did it. They will try and teach you, they will drive it into you, but the Hacker boards and stuff, once you get there they will ask you, what is your latest exploit that you have…that is too old, we had that six months ago, and then you have to go and try to find a new one, or go and try to Hack into this website, if you can then you might get into this IRC chat room, you are not going to get their IP address, you are not going to get anything unless you give them something that they want. It is about information exchange.
>
> (Respondent 9)

It would appear from these comments that there is then a community, a network which can be engaged with, but it does not appear to have the same hierarchical power structure as that which is found within the underground Hacking community (Jordan, 2009). Respondents in fact struggled to identify what it was that united them as a group, or distinguished the ‘Ethical Hacker’ identity.

> It is totally diverse, we are from different backgrounds, I’m from a different background from all these guys, but there is something that makes these guys

> one… that makes us, that makes us one [pauses] erm [pauses] but I'm really sorry but I just can not put my finger on it , [pauses] I just can not get it.
>
> (Respondent 2)

> … all the people that do our type of work they are more or less interested in the same things. It is the type of who will laugh at long techy, techy kind of jokes and stuff and erm... but it is not obviously the kind of person who will spend 24 hours in front of a computer sitting there. I'm not too sure how I can explain it, but there is something about the diversity. It is not like 100% anyone can be this type of a Hacker, its not that you have to be a little bit sad, just a little bit not too much just a little bit to have a full, full interest in the whole Hacking computer security stuff
>
> (Respondent 7)

As well as the apparent distinctions in structure between the Hacking and Ethical Hacking communities, it appears that there is identification with both communities by some security professionals which we will explore within the following section. It would appear that dual membership of both communities is common so that there are clear overlaps between the two. Jordan and Taylor (2004) also note that we typically find that communities online, particularly those involved in Hacking, are not discreet, but in fact typically intersect.

This avoidance of underground culture was found to be common among the respondents who currently, or previously had worked in policing, security or law, and also among educational professionals. On respondent said that he was "… trying to stop them, not make friends with them" (Respondent 7).

The avoidance of Underground Hacking culture and communities by many professionals is possibly because of the need for legitimacy within their roles, although this reason was not identified by the respondents and may therefore be an interesting focus for future research.

5.12 Summary and Conclusions

One of the respondents in particular commented that the difference between an Ethical Hacker and a Hacker was quite subtle, and was difficult for him to pinpoint. He likened it to:

> …the difference between a manager and a leader, you know? You can become a manager, you can go to school and become a manager but leadership qualities are there, it is actually a quality, so I think that is what a Hacker is, … being a Hacker is a quality.
>
> (Respondent 9)

Despite the difficulty in pinpointing the differences and similarities, it became apparent that there are some clear overlaps between Underground Hackers and Ethical Hackers, as well as there being a number of clear distinctions. They may share knowledge, activities and behaviours but there seems to be a general agreement that:

> there are definitely two different types of people, there is people who have gone in with an interest in computers and that is their background and they have thought I'm going to push towards computer security, and there are the people who have been interested in computer Hacking maybe as teenagers like script kiddies and they want to advance these skills…there are definitely two different sets of people.
>
> (Respondent 12)

This is borne out in the findings of this research.

Ethical Hackers indicate that they see Ethical Hacking and traditional understandings of Underground Hacking as being different in terms of the mindset, the motivations of individuals involved, and also the type and extent of the socialisation that they have. Socialisation is of importance as it creates the normative rules by which behaviour is guided; early socialisation within the computer underground seeming to have a particular bearing on the likelihood of later involvement in criminal activity and early discipline increasing the propensity to follow the law as will be discussed in the following chapter. It would appear that education does not make you a Hacker, and also that being an Ethical Hacker does not necessarily ensure that people will follow the law, or in fact that they will behave in an ethical way (which will be further examined in the following Chapter). It is interesting to note that those without underground affiliations see the employment of those with criminal backgrounds as being acceptable, and even beneficial to the sector, while those who admit to previous criminality acknowledge that this is problematic because of the potential impacts upon their employers, their customers and also their colleagues. Those with criminal backgrounds or affiliations may have a heightened awareness of the risks that are entailed for the employer, and therefore do not see this as being a rational choice to make.

It is also apparent that there is a clear social structure and organisation within Ethical Hacking as there is in the underground community, but that this is not hierarchically structured around power as in the wider Hacking community, but rather enables information sharing, training and support. Not all Ethical Hackers involved in this research chose to engage with Ethical Hacker networks.

Respondents suggest that that they perceive there to be two distinct groups of people working within the field, but also that some Hackers cross the line from one group to the other, while others choose to sit on the line, or to move with ease from one community to the other on a regular, and often daily basis, having affiliations with both,

In the next chapter we will examine the socialisation and the different normative and philosophical ethical approaches which impact upon the behaviour and the choices of the respondents. This is important as these form heuristics which act to bound the rationality of decisions made.

Chapter 6: Cyber-ethics and the Ethical Hacker

> I think your morals define your ethics
>
> (Respondent 12)
>
> I think that as far as ethics are concerned there is a very, very grey area between... You might think something is right and I might think something….the same thing is wrong.
>
> (Respondent 7)
>
> I think that if you take a look at it using a normal distribution curve, the shade of grey is in the middle, you know, the whole 90% in the middle, that is how grey it is. There is so much ambiguity; it is a very, very fine line. You can do it [cross the line from Ethical Hacking into illegal forms of Hacking] just like that, it is just so easy.
>
> (Respondent 2)

6.1 Introduction

In chapter two the available literature and typologies relating to the hacking underground were examined. In chapter three we examined a number of approaches to ethical decision making. This revealed that it is possible to understand the nature of underground ethical hacking (hacking that is ethical, but that is not carried out by hackers who have been employed to use their hacking skills) within the three meta-ethical approaches detailed in chapter three (namely virtue ethics, deontology and utilitarianism).

Within this chapter we will examine the relationship between these three approaches to ethical decision making and the ethical hackers who responded to this research and will show that it is possible to understand nature of ethical hacking also through these three meta-ethical approaches.

Cyber-ethics has been described as being "…the study of moral, legal, and social issues involving cyber-technology" (Tavani, 2007: 3). Respondents have indicated in their interviews that morality and ethics are important to them in both their work and in their personal lives. They suggested that they may apply different normative or meta-ethical approaches, or combinations of them in different circumstances.

Chapter Six will outline the main theoretical approaches to morality and ethics and will go on to examine the relationship between these and the motivations of the Ethical Hackers who have been interviewed for the purposes of this research.

Although much of the existing literature will suggest links between ethics and the law, and often tends to describe the law as a branch of normative ethics, it has been decided that the legal framework and its development should be dealt with separately to ethics as the respondents in the study see these as being discrete issues. As one respondent stated "…things can be ethical and illegal. Things can be unethical and legal" (Respondent 6).

6.2 The Impact of Socialisation upon Hacking Behaviour

The following sections will examine the social structures which create a frame of reference, informing the behaviour and social organisation of the respondents.

The initial assumption was that a fairly homogenous group of individuals were engaged in Ethical Hacking and that these were all drawn from a background which involved Hacking as part of the 'computer underground. During the initial fieldwork it very quickly became apparent that this assumption was incorrect, and that there are two clear routes into Ethical Hacking, and that these influenced the respondent's views, decisions and behaviour; these are a product of either socialisation with the Hacking community, or within the security industry. Socialisation and moral education in the home, through religion, and in formal education, have also been found to have a significant bearing.

Respondents all agreed that background and previous socialisation were essential in formulating their various views on the nature of right and wrong, and the frameworks which influenced their choice of behaviour when presented with a moral, legal or ethical dilemma. As previously discussed, this acts to bound the rationality of decisions made. One respondent described the background and socialisation Hackers as clearly distinguishing the Ethical Hacker from the Underground Hacker. He said that "… the only thing which really differs is probably what they have taken from their background which they have come from" (Respondent 22).

Other respondents talked more specifically about the factors within their own backgrounds which they felt had been influential in the choice that they made to use their skills in a legal way. The following comments reveal that family, work, and religion were of importance:

> …my upbringing, obviously, sort of parents, in later years my work; I worked as a security guard for a couple of years and with that you re upholding ethics and that as well. I guess I have been driven that way it has just been part of me
>
> (Respondent 12)

> I suppose it is the way you are brought up really, I think as far as ethics, and morals, and everything else, it totally comes down to how you are brought up, how you grew up, and with who, were you stealing? If you were stealing you are going to steal now, If your momma slapped you when you stole, then you know that stealing is wrong, and you still know that stealing is wrong ten years from then, it actually comes straight down to your roots
>
> (Respondent 2)

There would be nothing stopping me [from using her talents to break the law] I guess, but I was given a [pause] how can I put this? [pause] like a sense of good and bad, a moral way of doing things, mainly from my mother [laughs] I would never break the law, she'd kill me! [laughs] but also my faith has had a big part to play in my working life…

(Respondent 7)

…when you are a kid, and you script kiddie, you like computers, and there's a guy with a hotmail or a yahoo messenger account and there's a guy with an MSN account, so I remember in those times there was loads of erm, little programmes that used to come out, and so I used to find it kind of nice that you can get this programme and lock your friend out of hotmail or block your friend out of yahoo, so it was pretty cool then, and then as time went on I really thought that that was actually a place to try and get yourself developed in. Originally I didn't want to do a course in cold forensics and pen testing, because actually I was doing sciences, and math and physics and stuff, and I figured out that maybe computing might just be the thing, so I left [names a University], and came over to [names a University] to do the penetration testing course and forensics course and its been going on since.

(Respondent 9)

It is a legal background as a police officer for the last 25 years, and I have worked in this field for the last five years

(Respondent 14)

There are more people who have gone in on a computer background; I think that changes how they see things

(Respondent 8)

I was doing a course here, at the University, and I went on a placement, with a security company…

(Respondent 19)

I worked in [names a client company] legal software department actually writing legal books and converting them onto the very first IBM XT's in the early eighties so that is how I got interested in computers. Going the other way was never on the table

(Respondent 4)

Ultimately, I am in the business of law enforcement. My reality is I know the law

(Respondent 14)

Although socialisation is conducted by a range of different agencies, in different ways and with different outcomes most respondents talked about it when asked how they made decisions about how to behave in terms of what is or is not ethical behaviour. Thus we may understand socialisation as a generative mechanism which underlies the choices made by Ethical Hackers, even though this manifests itself in different ways, and not every respondent identified it. The fact that most respondents described some element of their socialisation means that we can understand it to be a 'demi-regularity' (Lawson, 1997) and although we cannot extrapolate from this, we can suggest that it may be an underlying generative mechanism in the formulation of ethical choice. Socialisation creates heuristic boundaries which influence choices made.

The following section will discuss normative approaches to ethics for Ethical Hackers, which will be referred to again within discussing deontological meta-ethical approaches, as these pertain to following rules.

6.3 Normative Approaches to Ethical Hacking

Most of the literature that has been published on the topic of computer ethics has taken the normative approach (see also Parker, 1979; Forester and Morrison, 1994; Johnson, 1994; Bowyer, 2001; Hester, 2001; Spinello, 2011) They tell us what is acceptable behaviour in relation to computer technology, and provide a clear set of standards to be followed.

Normative ethics can be considered as being the 'applied' branch of ethics. It prescribes how an individual should act in a particular set of circumstances, and therefore may be considered to be more closely related to systems of morality than can meta-ethical approaches. Normative ethics includes social norms, formal and informal rules, values and also standards of behaviour which may be variously codified as policies, professional or organisational rules, or as legislation. Examples of normative ethics would also include business, medical, or other professional ethics. In the case of computer ethics, these professional standards have been clarified within an number of national and International standards associated with professional bodies including, for example, the Association for Computing Machinery: ACM Code of Ethics and Professional Conduct; British Computer Society: BCS Code of Conduct and Code of Good Practice and the IEEE: IEEE Code of Ethics and also the Computer Ethics Institute: Ten Commandments of Computer Ethics.

While many Ethical Hackers will join these professional bodies and follow the guidelines provided, some of the respondents indicated that they felt that choosing the right course of action was not their responsibility, rather, this was the responsibility of the employer so that "…it is down to the business to make sure that it is ethically the right thing to do" (Respondent 12).

Many of the respondents feel that Ethical Hacking is made legal because it is authorised (which is the case according to section 1 of the computer Misuse Act 1990). This authorisation was thought to be in the form of permission from the employer. One respondent stated that in his opinion "...you are on the side of the law due to the contract" (Respondent 8). Others concurred with this perspective, stating that "…to get authorised, you have to get employed" (Respondent 12) and that "I would stick by the legalities and what you've been contracted to do" (Respondent 12). The perception is therefore that if you only do what your employer tells you to do, and what your contract prescribes, you can not fall foul of the law.

Respondents all perceive a clear distinction between Hacking and Ethical Hacking in that Hacking is illegal, and Ethical Hacking (in the academic sense of the term) is legal (those with affiliations to the Hacking underground also described for me instances of illegal Hacking which they perceived to be ethical). The discussions during interviews slid easily and frequently from law into ethics and morality and back again, indicating that there is a link between ethics, morality and the law. They are all measures of what is 'right' or 'wrong' for the Ethical Hackers that were interviewed. As previously discussed, morality and ethics are also clearly associated with authorisation for some of the respondents:

> At the end of the day if an Ethical Hacker's doing something that if they had not been told to do it or if they had not been asked to do it, and had not signed a contract and things, it would be immoral and unethical what they were doing.
>
> (Respondent 12)

Respondents often associated these ethical and moral notions of what is right and wrong with legality, and also often described legality as being associated with ethics; thus behaviour was deemed to be legally and ethically acceptable if sanctioned by an employer, thus it is the employers' responsibility to decide upon what is right and wrong on behalf of their employees. The responsibilities surrounding ethics and the law were with the employer for some respondents.

6.3.1 Ethical Hackers and the Legal Framework: Conformity and Dissent

Interview data has revealed that legality is a primary concern to the respondents, and that it shapes the ways in which they view themselves and others, both Ethical Hackers and Underground Hackers. The law defines for them how they should act and is therefore understood to offer a normative framework for behaviour in the same way that professional standards do. Some respondents described conforming unquestioningly to the law, some were found to conform whilst privately criticising, and others were dissenting or acting with disregard. This section will focus on how the respondents perceive and how they respond to the law, whether or not they choose to adhere to it, and how and why these choices and views are formulated.

According to Lipton (2010), law may be the most effective way of dealing with cyber-crime, but in order to have an impact, this must be current law which clearly defines the behaviours that are being legislated against. The individual actor must also be aware of the law in order for it to have an impact upon their decision making. Respondent 2 is illustrative of this issue. He had no knowledge of the legislative framework, yet was employed full time as a Certified Ethical Hacker, and had been through several courses of education. He states:

> I am not that informed as far as the law is concerned about Hacking. I do not know if there is much stuff about Hacking, with the law is there?
>
> (Respondent 2)

Without Ethical Hackers having an awareness of the expectations that are codified in law, it clearly cannot perform its normative function, and for this reason the legislative framework must be included within the curriculum of formal courses of education and training as well as within professional standards, both of which must be regularly reviewed in order to remain current.

There are currently three key approaches to legislating for digital crime, firstly there is the use of existing laws and statutes, secondly the amendment of existing laws and statutes and finally, the creation of new laws and statutes

This chapter will go on to consider the usefulness of each of these three approaches in relation to their ability to deal effectively with a variety of types of computer misuse offences, making use of illustrative case examples in evaluating these. It will then progress to a consideration of the complexities of the relationship between Ethical Hacking and the law, and how Ethical Hackers perceive and how they respond to the legal framework.

Wall (2007) identifies three types of cyber-crime that require legal remedy. These are: traditional crime (crimes which can take place with or without the aid of a computer, and therefore prosecutable under traditional statute), hybrid crime (crimes which can occur without the aid of a computer but which are altered by the use of a computer and may therefore require amendments to statute, or be covered under new statute, McQuade (2006) refers to these as 'adaptive' crimes) and finally true cyber-crime (crimes which require computers to be included, and may therefore require completely original legislation). Please see chapter three for a full discussion.

The following sections will deal with normative professional standards and the law; philosophical ethics will be dealt with separately later in this Chapter.

Common among the Ethical Hacking students and educational professionals interviewed for this research is the view that the law should always be followed, because "Ultimately…the law is black and white" (Respondent 4) but with the acknowledgement that the law may not be adequate. As respondent 9 states of the Computer Misuse Act 1990 as amended by the Police and Justice Act 2006 - "Well that is not enough is it, well that is just not going to work" (Respondent 9). Many of the respondents referred to what they described as a 'grey area'; "…there is a grey area, and a policy vacuum between the law and what is ethical..." (Respondent 10).

This ‘grey area’ is seen to occur for a range of reasons; firstly, it is reported that the law quickly comes to be obsolete due to rapid technological change.

> The grey area... has to do with the legal side of things and the law not having caught up with the technology. That creates a grey area; obviously a policy vacuum…there is the Computer Misuse Act. It is just so out of date…the new technology changes so quickly; the skill set changes so quickly that the legislation is just not keeping up with it.
>
> (Respondent 16)

There are issues created by the delay in creating new laws; often law enforcers and policy makers are acting reactively and the processes involved can be slow as problems will first need to be identified and then will need to be discussed and debated before being legislated for. There are a number of stages involved in creating new laws or making amendments to existing laws, these stages are time consuming, and are not always successful in achieving their desired outcomes. One respondent highlights this issue by stating that “…because of the lag in legislation there sometimes is a gap”, he then goes on to also say that “…sometimes the law is just wrong.” (Respondent 16)

In explaining how the law can be ‘wrong’ he goes on to suggest that there are also issues relating to the conflicting nature of some pieces of legislation for dealing with the misuse of computers. He states that:

> … sometimes the laws are contradictory. You know, so things like, I mean, The Computer Misuse Act, do not necessarily align with the Obscene Publications Act, so there is a contradiction there for example.
>
> (Respondent 16)

The law may also be vague, it may be unclear, or may be ambiguous:

> There has been a handful of people convicted under the Misuse of Computers Act, and I know that, erm, it is a very wishy washy piece of legislation

(Respondent 23)

One student of Ethical Hacking described the following experience which is illustrative of the perceived ambiguity within some of the present legislation, which could cause confusion about which activities are legally sanctioned, and which are not:

> …we got a computer lawyer in and he gave us a talk on the misuse act and when we put the questions to him is port scanning illegal, he could not answer. Because it does not fall under the Computer Misuse Act you're not going in with an intent of doing anything but then there are still people who have been prosecuted because they have said that you were port scanning for a reason you weren't just doing port scanning for pleasure.
>
> (Respondent 8)

The law can not, therefore, be understood to provide clear normative boundaries to inform decisions about which behaviours are acceptable, due to its ambiguous nature.

As well as the issue of the different cultural and social views on criminality which exist in different countries, there are also universality problems with legislation, which in a global industry such as Ethical Hacking can cause jurisdictional problems. As one Ethical Hacker points out: "Once you go cross border there are a lot of grey areas. What is illegal in one country is not necessarily illegal in another" (Respondent 10).

This issue has previously been recognised by the Law Commission (1989):

> A Hacker, with or without dishonest intentions, may for instance sit in London, and through an international telephone system, enter or try to enter a computer in New York or vice versa. More complex 'chains' involving computer systems in a number of countries before the 'target' computer is accessed are entirely possible.
>
> (Law Commission, 1989 as cited in Fafinski, 2009: 42)

The problems are seen to have emerged due to the fact that the technology used in commissioning of cyber-crime can transcend national boundaries in a way that the legislation and the regulatory bodies can not. This is suggestive of the need for an international approach to dealing with cyber-crime, although this would be problematic due to the varying cultural and social norms across the globe.

> The rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating new phenomena that need to become the subject of clear legal rules but that cannot be governed satisfactorily, by any current territorially based sovereign.
>
> (Johnson and Post, 1996: 4)

Sometimes illegal activity does not just cross state boundaries, but is also actually state sanctioned. The state sanctioned hacker may work in national security, or be employed as a freelance employee of a government agency. Respondent 10 described the ‘grey area’ of state sanctioned Hacking. He saw this branch of ‘Ethical Hacking’ as making up a significantly large section of the computer security industry. He states that “… there is the grey area of legal Hacking, you know, state sponsored …there are lots and lots of state sponsored Hackers” (Respondent 10).

With this type of Hacking behaviour the perspective on whether a ‘crime’ has been committed is related to personal and cultural perceptions, and may be related to whether you belong to the country of origin or of attack. The legal dimension is superseded by the authorisation of the state. Unfortunately, although this type of Hacking is referred to in the literature and by the respondents to this study, the sampling method employed, combined with the highly secretive nature of the work, did not allow access to any Ethical Hackers of this type, which would have added rich data to a discussion of how decisions are made regarding ‘right’ and ‘wrong’ behaviour. This may therefore be an interesting topic for future research.

Hacking is clearly defined by its legal dimension rather than by its relationship to morality or ethical systems as it is the authorisation, or lack of it which defines it as being either Hacking or Ethical Hacking, however, as has been discussed, the legality of Ethical Hacking has also proven to be problematic. An example of this is that there are potential cases under the new revisions to the Computer Misuse Act (CMA) 1990 under the Police and Justice Act (PJA) 2006, where an Ethical Hacker may break the law in pursuing his work or research (please see Chapter Two for a full discussion). An examination of the amended CMA would indicate that it is not always easy to stay within the law, and in fact, many Ethical Hacking professionals may frequently act against the law in their day-to-day work.

It is generally agreed that in order to be an Ethical Hacker the intent must be to do good for society, and to stay within the law. Some of the respondents however perceived status to be more closely related to Hacking, and so may get more emotional value from acting illegally.

Students and educational professionals agree that even if the law is out-dated it must be adhered to in order that skills and activities normally attributed to the Hacker may be defined as 'Ethical Hacking'. One educator within the field suggested that the Ethical Hacker should "…always work within the law. Always stay within the legal system… if you are breaking the law then it is Hacking." (Respondent 10)

This illustrates that the respondent has the perception of there being a clear distinction between the activities of Hacking and Ethical Hacking, this distinction being drawn by the legislative frame-work. This was found to be a common view among the respondents and within the literature.

Some of these respondents, mainly those with current affiliations with the computer underground, did not see illegal activity as being an issues as is indicated by respondent 2 who states that "…It [hacking into some-one else's server] may be illegal in this sense or that sense, but I really do not see the problem." (Respondent 2)

Those Ethical Hackers who have entered the field from an underground rather than an academic or professional background are not so 'black and white' about the law. One respondent gives examples of crimes he would and would not commit:

> So taking credit card details is something that I am going to say I can not do. But one thing I could do is I would get into one of those guys networks, and I would find out that they have got, like, four servers, and um, one of them is virtually unused.
>
> (Respondent 9)

They generally excuse what they see as 'victimless' crimes and therefore rationalise their behaviour to themselves (Sykes and Matza: 1957) whilst thefts, where it is more difficult to deny the victim (ibid) are not seen as being acceptable. All of the criminal actions that were described in the interviews could be rationalised as being not harmful to others. If any of the respondents had engaged in thefts this was not admitted during the interviews. The ethical considerations would appear, for some Ethical Hackers, to have more of an impact on their behaviour than the legislative framework.

Parker (1979, 1998) suggests that Hackers need to rationalize their crimes in much the same way as more traditional kinds of criminal (Sykes and Matza, 1957). One respondent to this study suggested that being an 'Ethical Hacker' in the underground sense of the term (illegal, but for an ethical purpose) was itself as a form of rationalisation of criminal behaviour

> They need to justify their actions, for whatever reasons, erm, okay, I am Ethically Hacking into this, or I am doing this for whatever reasons. Okay I am Ethically Hacking into this, or I am Hacking into this because I believe we should deface this page because we should save the animals.

(Respondent 2)

As has been discussed, another serious issue is that the law can often be difficult to enforce with regard to cyber-crime which offers a unique set of challenges in identifying the crime, pursuing the perpetrator, collecting the evidence, and proving the case in court, if indeed the crime falls within the particular jurisdiction in question. One respondent with a history of policing found this particularly frustrating, stating that this caused problems for policing of cyber-crime because:

> …ultimately, whatever is on the computer is on the computer, but there are a hundred and one ways that that get on to the computer...unless I am actually looking over that persons shoulder; I can not say whether it was that person who actually typed it in.

(Respondent 14)

The legal framework however is only one of four approaches that can provide normative controls (Lessig, 1999; 2001; 2004; 2007) as was discussed in chapter 3. The following sections deals with meta-ethical approaches, and the influence that these have upon Ethical Hacker decision making.

6.4 Meta-Ethical Approaches

Meta-ethics is described by Stamatellos (2007) as being a form of theoretical ethical reasoning, and pertaining to the nature of moral obligation and duty. It describes for us the nature of, and basis of normative ethics. It attempts to describe the essence of right and wrong; it is a purely philosophical position and describes how we should approach or perceive decisions or thought. It is outside of ethical practice, pertaining more to ethical thought or reasoning. Meta-ethical thought informs normative practice which was discussed in the previous Chapter through an examination of law, rules, and professional standards.

Meta-ethical approaches may cover a very broad spectrum, narrowing to a very specific prescriptive set of normative professional standards. There are three main meta-ethical approaches which will be considered; these will now be explored in more depth with reference to the responses of the interviewees who have been interviewed for this research. These are virtue, or character ethics, duty based, or deontological ethics, and teleological approaches or consequentialism, which usually tend to focus on utilitarianism rather than egoistic or altruistic approaches. They focus on intent, action and outcome. It will be suggested that the motivation and socialization of the Ethical Hackers who have been interviewed largely characterises the meta-ethical approach which they take, and their perception of, and adherence to, the normative ethics by which they must guide their behaviour, in order to define themselves as Ethical Hackers.

We are now in a position where it is possible to consider the three main meta-ethical positions and their relationship to normative ethics, alongside how these have shaped the reasoning and behaviour of the ‘Ethical Hackers’ who have responded to this study.

The first of these approaches has been described as the ‘virtue’ approach and focuses upon the intent of the actor as the key defining characteristic of whether something may be defined as being ethical or not. This approach was favoured by Aristotle (Hope, 2010) who felt that only good intention can lead to good action. The approach is individualistic being based upon the personal actor.

The second major approach is the Kantian or deontological approach. It is based upon systems of morality and justice which should be applicable to all (Rawls, 1971) rather than individualism; it is therefore a universalistic duty based approach. Any action is justifiable if you wish it to be applied in equal measure to all; justice is related to universality.

The third major approach is the most well-known. Rather than intent or action, it focuses on outcomes, or consequences. The most well recognised consequential perspective on ethics is the utilitarian approach. Rather than seeking universality in moral judgements, the approach advocates trying to create the best possible outcome for the greatest number of people and is generally associated with the work of Jeremy Bentham (1781) and J. S. Mill (1806-1873).

These three meta-ethical approaches can neatly be arranged into what we intend to do, what we actually do, and the outcomes of what we do, therefore, INTENT, ACTION, OUTCOME, and can be linked to Underground Hacking typologies, as was described in Chapter Three. The types of Ethical Hackers, based upon their socialisation, tend towards certain of these ethical stances. In the following sections each approach will be applied specifically to the respondents of this study in order to show that these meta-ethical approaches with influence the decision making of Hackers and Ethical Hackers provide a useful framework for understanding both Underground Ethical Hacking and those who are employed as Ethical Hackers, and therefore creating a useful addition to the typologies that were discussed in chapter two. It should be noted that these may not be ‘pure’ types, and some overlap may exist between the categories presented in table 5.

	Underground Hacker	Ethical Hacker
Virtue/Character	‘True Hackers’	Educators/Students
Deontological	FOSS Hackers	Legal/ Security Personnel
Utilitarian	Hacktivism	Underground affiliated

Table 6.5 Meta-ethical Approaches to Ethical Hacking

6.4.1 Virtue/ Character Ethical Hackers and moral development through education

There is a tendency among the respondents who have been socialised into non-deviant social norms and then have later encountered Ethical Hacking courses to describe being driven by a sense of personal integrity, or character virtue. This has been found to be common among both educational professionals and students on these types of courses, and they describe seeing this among their colleagues and student cohorts. Respondents were asked about their motivations because “The lack of complete control over behavior is not due to cognitive bounds of behavior but rather to motivational ones” (Selton, 2001: 15).

When asked about personal motivations and where these come from the common response is that it is a personal intrinsic approach and that this is developed through socialisation and shaped by lifestyle. One respondent listed the following as shaping his motivations when asked why he had chosen to be an Ethical Hacker rather than a Hacker: “Upbringing, family, education, culture, my role as a parent, all of those things shape the way that I am”, (Respondent 16). There is evidence here of his own personal socialisation having an impact, but also his “…role as a parent…” which would indicate the desire to set a good example for his children. He went on to talk about how it was important to him that his children did the right thing, but also that as a parent he would not want them to see him breaking the law, as this would reduce his parental authority.

Another answers similarly, but lists other agents of socialisation including family, and previous employment.

> …up-bringing, obviously, sort of parents, in later years my work. I worked as a security guard for a couple of years and with that you're upholding ethics and that as well. I guess I have been driven that way, it has just been part of me.
>
> (Respondent 12)
>
> I wanted to get involved…. erm…. I was going to be a lawyer but decided there was more money in being a consultant to lawyers so that is why I got involved with legal software. It's that kind of background where you know the law and people know you know the law…
>
> (Respondent 6)

There is perceived to be a very close relationship between ethics and morality, with the acknowledgement that the law should also be aligned but cannot always be. "…[Ethics and morality] are not quite synonymous but that line is, if not totally on top, it is very, very close." (Respondent 16), "…it is a very, very fine line…" (Respondent 10).

There is some agreement that this professional ethic is related to the formal study of Ethical Hacking, which leads to a more developed understanding of why rules are followed. There is also the acknowledgement that these kinds of courses can be wrongly perceived by academia, industry or wider society (BCS, 2008; please see also Chapter Five for a full discussion of courses of education and how they are perceived)

Students also note that they perceived that a sense of personal ethics can be developed through education. On stated that in his opinion "….people who have been through courses like this [Ethical Hacking Undergraduate Degree Course] would have a stronger ethical perspective than those who have not…" (Respondent 8).

This suggestion is supported by Kohlberg's (1976) ideas about moral development and sees this moral development as being developed through study on an Ethical Hacking course as has been previously discussed. Moral development leads to an acceptance of the law, even if there are perceived to be issues with it. It is inherent within stage3+ of Kohlberg's (ibid.) taxonomy that this occurs because of an acceptance of the social contract as being mutually beneficial to all of society.

Not all students will leave with this ethical stance, or this level of moral development.

> …there is definitely two different types of people. There is people who have gone in with an interest in computers and that is their background and they have thought 'I'm going to push towards computer security', and there is the people who have been interested in computer Hacking maybe as teenagers like script kiddies and they want to advance these skills. Their motivation for the end of the course might be to find themselves a security job or in might be to be able to go away and Hack legally its hard dividing people but there are definitely two different sets of people
>
> (Respondent 12)

During courses of education it is not immediately apparent whether the individuals involved will use their skills legitimately:

> …there are the shared traits the shared skills and you cant decide which way they are going go in the future, you have got someone who could go either way and at the minute they are called Ethical Hackers because of the course they are doing but once the course finishes you can see them going off to become Hackers…
>
> (Respondent 12)

Some respondents indicated that their socialisation prior to and even during their time studying Ethical Hacking at university may have been more negative and that had increased the likelihood of them choosing to act illegally rather than legally. Respondent 9 suggested that he had negative influences in his childhood, and also while studying, he describes this saying that he "…had a couple of friends, obviously bad guys, I mean growing up you have a couple of bad friends, even when I was at the university as well…" (Respondent 9).

There is the perception that the opportunity to formally train and develop a code of ethics which maintains and passes on an industry accepted standard has resulted in there being a change in the industry so that it is now no longer common, or even necessary for a Hacker to be employed as a security professional as was common in the past:

> People that were breaching systems, particularly of financial institutions the banking institutions were employed, rather than, say the banks, saying you have breached our system; you know, come and fix it. That trend seems to have stopped. I do not know if that is because of the Ethical Hacking courses are contributing to that.
>
> (Respondent 2)

This is problematic because "…the reputational damage if somebody was employed as an Ethical Hacker and then they broke the law would be detrimental." (Respondent 18)

And this can have possible impacts for a wide range of industries because "…there are all sorts of different sets of employers that would employ an Ethical Hacker, whether it is a security system or an IT security system, or whether it is a government agency or a private forensics firm…" (Respondent 18).

Please see Chapter Five for a full discussion of employers of Ethical Hackers and what the roles of Ethical Hackers are within their employment. The discussion also covers the employability of ex-criminal Hackers.

The trend perceived trend used to be that people would Hack as youngsters, and then later on would change their career path and would utilise their skills legitimately:

> Well it seems to be that Hacking is a young persons skill and they are all locked away in their bedrooms, by the time they get to about 25 or 30 they realise that, oh, there is a life out there, or they get caught and they realise the risks that they are taking and they come to be more risk averse as they get older. There are a whole set of different reasons and rationales for changing. You only have to look at the likes of Kevin Mitnick, get caught who are put in jail, did some time, wrote a book and then comes out and says ooh, there's a lecture circuit here crying out for me and its much safer. They realise that once they get caught it is not a good place to be.
>
> (Respondent 16)

In fact desistance among offenders is more common than persistence among offenders, and it is noted that education, marriage and stable family life are among the factors that reduce persistence Soothill et al, (2009). Laub and Sampson (2003) note that stable work and career relation increase the sense of bonding to society and therefore decrease criminality. "Unemployed hackers reported a significantly higher number of hacking attacks than hackers who were employed", this is because "…hacking is a time consuming activity. Unemployed hackers simply have more time on their hands to dedicate to hacking" (Bachmann, 2010: 650)

Kohlberg's (1976) model is split into three stages, with two levels within each stage. Stage one is called 'Pre-conventional, and at the most basic level, we act, or obey rules, in order to avoid punishment; we are driven by the need to avoid negative sanctions, one Ethical Hacking student was clearly in this bracket stating that he "… wouldn't risk breaking the law and getting fined or jail or what ever" (Respondent 15).

In the more advanced level of stage one this is replaced by behaviour in which we follow rules in order to benefit the self. This could include staying on the right side of the law in order to remain employable. One respondent makes the following comment, which is illustrative of this desire to remain employable:

> I wouldn’t risk it [breaking the law], that would make it a nightmare to try to ever get another job ever again in this industry. There is plenty of people about without records that they can get instead. Nah, it is just not worth it.
>
> (Respondent 1)

This would suggest that in order for normative approaches to be adhered to, they must be underpinned by a meta-ethical understanding. This is idea would be

Virtue/character based ethical approaches may be criticised as they do not consider the impact of a lack of community homogeneity of variance in relation to morality, professional standards or other rules of conduct which guide our behaviour (Tavani, 2011). As we have seen, Ethical Hacking lacks this homogeneity of variance, and as we will see, this is because the respondents employ different ethical stances in their decision making approaches.

It would appear that while virtue is important, it is not the only factor at play here; the following sections will consider some alternative ethical approaches and their impacts on the respondents in this study.

6.4.2 Deontological Ethical Hackers and crime control work

Secondly we turn to deontological approaches. These focus on our duties under contract or under moral obligations.

Hackers who have a background in policing, or law, or in security tended to indicate that they perceived the ‘rule of law’ as being absolute. The secretary-general of the United Nations defined the rule of law as being:

> …a principle of governance in which all persons, institutions and entities, public and private, including the State itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated, and which are consistent with international human rights norms and standards. It requires, as well, measures to ensure adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, avoidance of arbitrariness and procedural and legal transparency.
>
> (United Nations, no date)

As we saw earlier in this chapter, these individuals tended in their responses to indicate that they are uncritical of the law and that they see it as being something to be followed under any circumstances, as the following comments illustrate:

> I can see where the grey area is, is it right or is it wrong comes into it, but from the law enforcement side of it, the law is black and white
>
> (Respondent 14)

> People can not just make up their own rules; that would be total anarchy. Some rules are better than no rules. There are proper channels if you think that it [the law] is wrong. You can not just have everyone ignoring it
>
> (Respondent 23)

> I hang my hat on the fact that if it is unauthorised it is illegal.
>
> (Respondent 5)

Deontological approaches stress duty and respect for authority and moral systems, but have been criticised for ignoring happiness as the intent based ethics do, and for ignoring utility, or usefulness of actions based upon a teleological understanding of ethical behaviour.

Deontology advocates rule following, which was discussed at length under the heading of normative approaches, and it also advocates rule setting, by acting in ways that we would want others to act. This was also apparent amongst those respondents who indicated that they did not and would not break the law. One made the following comments:

> I mean it's obvious isn't it? We have to be beyond reproach, I mean, if I am not doing things the right way what is going to happen when anyone finds out? I can't exactly do my job of making sure everybody else does what they are meant to if I am not going to, can I?
>
> (Respondent 5)

It was suggested that people need role models in order to help them to choose the right course of action. One respondent stated that he "think[s that] people need someone to look up to. They don't always pick the right people though" (Respondent 23). Interestingly, some individuals who had admitted that they were involved in criminality still wished to be perceived as role models. As the following comments indicate:

> I think us older guys who have picked the right path should be an example to the young ones coming up, but it just doesn't work that way
>
> (Respondent 19)

> You get some kid, and he doesn't know which way to go, but he has got the skills, he has got the ability. If someone is there at the right time to help him find his way, well that's all he needs. The trouble is that they aren't going to be likely to come across people like me who can show them the way…
>
> (Respondent 15)

Respondents shared in common a wish to act in a way that would have a positive influence on the behaviours, with some clearly being more suited to this role than others. This desire to be respected is to be expected among individuals who have community norms that value highly knowledge and status.

6.4.3 Consequentialist Ethical Hackers and the Hacking Underground

Utilitarianism, in common with deontology, can either focus upon either rules or upon acts. It is focused upon the consequences or outcomes of our behaviour rather than the motivations and intentions which drive our behaviours, or the actions in themselves. It is described as being a teleological theory in that the ends are perceived to justify the means, so that the outcome of an action justifies the process. In common with virtue or character ethics, utility stresses happiness, but seeks to measure this at a more societal and consequential level. An ethical decision carried out from within this approach would seek to balance the amount of pain caused by an act or rule in such a way that the pleasure the act causes outweighs the amount of pain caused.

Act utilitarianism is focused upon the outcome of a single act, which may be rationalised if pleasure or gain was caused for an individual, while not causing any harm to others (Prenzler, 2009). This may be termed 'hedonistic consequentialism". As described by respondent 9:

> Because I am not harming anything, nothing is going to happen. If I upload my movie to there [someone else's server], and five guys download the movie and then two days later I take it off, I do not see what the problem is. So I think that, obviously some people will say that it is not your server, you are not supposed to be doing that. It may be illegal in this sense or that sense, but I really do not see the problem.
>
> (Respondent 9)

This sort of rationalisation has been common among the Hacking (Parker, 1979; 1998) and phracking (Sterling, 1992) community who may justify using a phone line or an empty server with the rationalisation that 'no-one was hurt' by this action which has caused them some personal gain (Sterling, 1992). This is illustrated by the comment that "…it might be still breaking the law but it does not affect someone, so you think that is just the way it is going to be…"(Respondent 11). It would appear that harm to self and others and the benefits to self and others may be more important than the legal framework for some Ethical Hackers.

One respondent in particular talked extensively about how he made choices in relation to personal consequences and therefore was making a hedonistic utilitarian outcome based decision rather than one that was based in legislative normative or professional practice or standards. What is particularly worthy of note is that he was unfamiliar with the provisions of the Computer Misuse Act 1990. The following comments provide some examples of illegal activities that this respondent feels are acceptable as he does not perceive any harm being done to others.

> …Microsoft was quite easy to break into some time back before the whole live messaging thing, when it was still hotmail, you know, MSN, I found no problem getting inside there, locking guys accounts, doing this, and putting a little tether on the emails, It depends on why I am doing it. I could go in and lock your account today and the after two days I could re-open it. I do not see what the problem is. You might be pissed off, but I have still opened your account….
>
> (Respondent 9)
>
> ...I know that there is a machine, a sever that I can connect to by RDP and keep one or two pieces of code that I am writing, and each time wherever I am, if I am at a friends place, if I am at uni, I can just RDP into the machine, even at twelve midnight or whatever and then log off. Then after three months take it off. I do not see what the problem is… I mean as long as there is a purpose, a really good reason why.
>
> (Respondent 9)
>
> …I really do not see a good reason why I should turn down I guys server, and then he will turn it back on and I will turn it down, and then he turns it back on. I do not see why I should do that. I am not going to gain anything….
>
> (Respondent 9)

He indicated that he may try something once, as a challenge, but once the motivation is acted upon the behaviour is not repeated as the sense of challenge is reduced. Other respondents with underground links or origins tended to concur with this view.

> …I'll try it, it works, done. Tomorrow the guy's server is back up, why should I turn it off again?"
>
> (Respondent 9)

> …I'll ask myself if there is anything at the end of it. If there is nothing, if there is no good reason, then I am just not going to do it….
>
> (Respondent 3)

Rule utilitarianism would focus on the setting of precedents so that the behaviour becomes harmful only if it becomes a rule for behaviour which others also follow (Prenzler, 2009) and in the case of the example above may be the sort of argument we could expect from a communications company who own the exploited server, phone-line or other facility. They might ask 'what would happen if everyone does that?' It quickly becomes apparent that the companies would no longer be able to operate as they would lose the revenue which is due to them for the service. The consequences may be that the company, and therefore the service or facility that they offer, ceases to be available. If we go back to the basic utilitarian cost/benefit analysis we can see that the costs to a great number of people far outweigh the benefit to the few people who seek to utilise the service for free. It could be argued however, that it is unlikely that everyone will start to try to access a service for free. It is apparent that some of the respondents are aware of the companies that they exploit making these kinds of cost benefit analyses.

> …if these big companies lose out to one guy, I mean they lose one credit card or they lose £100 to one guy they are not really going to go to all that trouble to try to find me…if even they lose for example 50,000 credit card details they are not going to look for you, because it is just too expensive…
>
> (Respondent 9)

Respondent 23 was clear that he felt that 'not doing harm' was not the only factor to be considered, which he illustrates with the following example:

> I have spoken to Hackers, you know, Hackers, people who are breaking the law, and they have this belief that they have a right, a moral right, to go into other peoples property, and do whatever they want to do and I would equate that to you walking into my house, and sitting watching my telly and then saying well, I am not doing you any harm. *But you are in my house*…
>
> (Respondent 23)

The invasion of privacy and of territory is also then something that creates harm, but this harm is apparently not always a consideration.

Kizza (2010) further develops consequentialist arguments by suggesting that social utilitarianism is not the only approach which is used in making a teleological argument for rationalising behaviour. The above rule deontology may be rejected by either an egoistic or an altruistic individual, (as seen in respondent 9's actions as described above) who, rather than making a socially useful decision will either be self-serving, or self-sacrificing in their behaviour. Kizza (ibid.) also provides us with some useful ideas about the nature of some of the consequences to be considered. These may be psychological, e.g. isolation, or social, e.g. moral decay, or affecting both the individual and society, e.g. loss of privacy (as in the example above) or loss of trust. We may add physical consequences to this list as is the case where an individual is harmed or killed during medical testing which may be of great benefit to a great number of people, although this consideration is outside of the scope of this research.

Hackers will sometimes rationalise their behaviour by suggesting that this does good for others, rather than simply not doing harm. This is in common with the rationalisation of criminal behaviour by appealing to higher loyalties, as described by Sykes and Matza (1957). The respondents in this study showed an awareness of others, and the desire not to do harm, however there were no indications that they were hacking to try to create positive outcomes for others. Although this is not seen within this research in Ethical hacking where the Hacker is employed, some Underground Ethical hacking, and notably within the FOSS community, and also Hacktivists who engage in behaviours which they perceive to be for the benefit of others.

6.5 Conclusion

There exists a set of professional standards by which Ethical Hackers behaviour may be normatively controlled. These professional standards are optional, relying upon the individual to have membership of a professional organisation. It is notable that none of the respondents in this research described membership of any professional body as a factor when asked how they made decisions about what was right and wrong, good or bad, legal or illegal, ethical or unethical. It may be useful for the industry to require membership of these bodies in order to ensure a more uniform following of the standards that they provide. Some employers do currently request this. This would provide a level of assurance to the users of the service that the people that they employ to provide them with the service are operating within a clearly defined set of industry standards.

Ethical Hackers who previously have had, or presently have links to the computer underground tend to be more critical of the law, and for this reason they were less likely to work within it. Those with professional backgrounds in law, policing or security tend to be much more likely to believe in and uphold the law, even where they recognise there to be shortcomings. This may be because of the need to protect their legitimate reputation, as well as the socialisation that they have received providing a form of informal social control which would provide a set of heuristics to guide decision making.

The respondents to this study have indicated that the way that they perceive the legal framework, and whether they choose to operate within it or to disregard it, is related to the way in which they entered the field, the way their careers have developed, and the sources of their socialisation. This has been a combination of peers, family, education, work, and religion as was discussed in Chapter Five. Upbringing was frequently commented on and was thought to be of particular importance. Again these provide a set of heuristics which will reduce the level of actual reasoning that is involved in decision making.

Those with connections to the underground are critical of the law and ‘flexible’ in their approach to working within it, seeing personal ethics as being more important in deciding whether behaviour is ‘right’ or ‘wrong’. They indicate that they would generally not wish to engage in activities which they perceived to be harmful, and were happy to break the law only if they did not perceive any harmful outcomes, particularly if the activity was a source of personal satisfaction or pleasure. Educational professionals and Ethical Hacking students indicate that they are aware of a range of problems with the law, but suggest that the law must be upheld, and should be revised so that it is fit for purpose rather than being ignored. Those with legal, security and policing backgrounds are completely uncritical of the law and see the law as the ultimate measure of whether something right or wrong. They closely align law, ethics and morality. It is apparent that while there have been a number of prosecutions; the law is at best vague and ambiguous, despite a number of revisions which would support some of the criticisms levelled by the respondents to this study. The law, therefore is failing in its normative function, except where people choose to uphold it because they have been socialised to do so.

In interviewing so called Ethical Hackers about their ethics, morality, motivations and behaviour is has become apparent that ‘Ethical Hackers’ can be divided into three different groups based upon their ethical understanding. Virtue/ character based Ethical Hackers seem to be drawn from an educational background either as educational professionals or students, and have an advanced level of moral development based upon their previous socialisation. Duty based Ethical Hackers tend to have a background in law or policing and follow the law because they believe in the rule of law as being absolute. Consequentialist Ethical Hackers make their decisions based upon personal or social gain, compared against personal or social outcomes. These Hackers tend to have a connection to underground Hacking and often admit that they have underground, criminal or deviant associates. Some have been educated, but despite this they do not see rules or laws as absolute, but rather as social constructions to be circumvented. A personal set of ethics seems to be of more importance to this group. Please see also chapter 5 for a full discussion of the relative impacts of community affiliation and formal education.

The differentiated following of these types of ethical behaviour shows that there are different ‘boundaries’ that restrict the reasoning process of the individuals involved. These are related to the circumstances of the particular event and the social context and the individual frame of reference within which the event takes place.

It would appear that ethics and morality are of clear importance to the respondents; however it is problematic that they do not appear to share a clear understanding of the meaning of these concepts. It may be more useful to state that they are all concerned with notions of right and wrong behaviour, even though they all employ different ethical frameworks to provide them with a standard for this. It is however apparent that there is diversity in the systems of thought which contribute to understandings of right and wrong behaviour amongst Ethical Hackers, and that they utilise a wide variety of ethical frameworks to make such decisions, so that there is not uniformity in understandings of ethics, or ‘ethical’ behaviour amongst Ethical Hackers.

From the responses in this research it would seem that when you hire an Ethical Hacker you can be assured that he will be ‘ethical’, but you have no way of knowing what type of ethical he will be.

Meta-ethical approaches then clearly act as heuristics in decision making, but these manifest themselves in different ways according to socialisation.

Chapter 7: Conclusion

7.1 Introduction

This Chapter will provide an overview of the research findings in relation to Ethical Hackers, their motivations and their conduct. Consideration will be given to the ways in which Ethical Hackers have been found to be similar to and also to differ from, Underground Hackers. This will include their views on ethics, morality and the law, how these views developed and how they inform their decision making and their behaviour. This concluding chapter will then go on to discuss the impact of the research for employers, both private and public sector, as well as a range of other interested stakeholders including educators and the individuals involved, and then to consider the implications raised by the findings for further research within this newly emerging field of study.

7.2 Rationale

This research was undertaken in order to examine a new and exciting field of study which has not been previously examined in relation to the rational processes involved in behavioural decisions. While there is a wealth of literature which typologises Hackers and more recently which attempts to explain their criminality, this work offers an original contribution to knowledge by attempting to begin to understand the nature of Hacking behaviour which is not illicit, and to understand this behaviour in relation to notions of right and wrong, as perceived by those within the field. This has been examined here by utilising a framework of meta-ethical philosophical approaches, and is understood in relation to the development of the legal framework which criminalizes the Hacking behaviour. It is therefore of importance to those individuals working within the field, to employers within both the public and private sectors, and also to those who buy the service, either as organisations or as private individuals and to those who engage in education and training within the field. This research also has implications for the Criminal Justice System as a whole, and in particular for the judiciary who have a significant role as buyers of the service, as well as in controlling criminality.

Much of the information which emerged from the study about the nature of hacking, Ethical Hacking, and the differences and similarities between them came from questions which were initially meant to ensure a shared sense of understanding between the researcher and the participant. These turned out to be of importance to the analysis which followed, much more than was initially anticipated.

The research also set out to gain an understanding of the social structure of Ethical Hacking social networks, and how these relate to the wider Hacking community. This was partially in order to gain a better understanding of a social group that has not been previously studied in terms of its community, but also in order to examine the impact of the social network upon decision making processes.

7.3 The Nature of Hacking and Ethical Hacking

The term ‘Hacker’ is much contested as discussed in Chapter Two and in Chapter Three. Its definition appears to depend on a number of factors, and most importantly whether it is perceived as being a verb, so that we see ‘to hack’ as being an activity, or whether we see ‘the Hacker’ as being a type of person. Their have been a number of attempts to profile the hacker and these seem to describe a variety of people in a variety of contexts. For this reason the interviews commenced with a discussion about what these terms mean to the respondents, as well as how this relates to the idea of Ethical Hacking. Despite the conflicting academic discussions a number of common threads emerged. The hack is perceived to be an activity where software is somehow circumvented; the hacker is a person who has a mindset which allows him to do this. The Ethical Hacker, as we have used the term in this research to describe a person who hacks with authorisation, may be more accurately described as a Legal Hacker, as the term Ethical Hacker is used by respondents and within the literature to describe both those individuals who hack legally and those who hack for an ethical purpose even if their activities are illegal. The term Ethical Hacker has been adopted by academia, by the individuals involved and by industry; however this is a source of confusion. It has particularly been criticised within the debates which surround the use of the term within the titles for courses of education.

Hacking and Ethical Hacking have been found to have a number of clear correspondences, but also some characteristic distinguishing features. They can be considered to be linked activities and have some shared social networks, but they are most certainly not completely synonymous with one another.

Hackers and Ethical Hackers would seem to share a range of motivations in that the respondents have indicated that they are driven by a sense of challenge, the desire for prestige, and a desire to learn and to improve their skills. Both groups share in the same behaviours, expertise, and knowledge, although the behaviour is legally sanctioned in the case of Ethical Hackers and not for Hackers in general who carry out the same actions, but without authorisation.

Both groups have been found to have some level of social organisation, although these function quite differently. In the underground community, Hackers generally organise themselves in a hierarchical fashion, with information sharing organised through power structures so that only those with perceived levels of similar knowledge are allowed access. Information is shared in order to gain status, or in order to trade with other Hackers. For the Ethical Hacker, the social organisation follows a more ‘flat’ structure, members are happy to share their knowledge and information with one another and to try to improve their colleagues and their networks levels of ability. Respondents felt that there was something which united them as a group, but found that it difficult to define what this was.

Also of interest is that there are clear overlaps between the two communities, with many Ethical Hackers indicating that they move between the two communities with ease and on a regular basis, often daily. This is in order to enable them to keep up with latest advances so that they can be effective in their work, but also so that they can continue to engage in criminal activity. Those that move between the two communities have tended to have an ‘underground’ background before they were employed as Ethical Hackers. It is also worthy of note that although all of the respondents were aware of these communities, some did not engage at all with either. Those who were in management or educational roles, where they were not involved in frontline security seemed least likely to engage with social networking – for Ethical Hackers social networks seem to be engaged with out of necessity, and not out of a sense of community or belonging as found within the underground community.

Ethical Hackers are unlike Hackers in that they can come to be defined as such through their education, and through the legally sanctioned nature of their activities and behaviour; this is not the case for Hackers in general where being defined as a Hacker is related to skill, knowledge and status, rather than to qualifications and employment in line with the Hacker Ethic as defined by Levy (1984). This means that many of the respondents were clear that being employed or educated as an Ethical Hacker, does not, in their opinion, qualify an individual as a ‘Hacker’. They felt that while Ethical Hacking was clearly associated with what you do, Hacking is more about the mind-set that a person has, it is about how you reason and what you know, rather than how you act. Despite this, most of them still talked about the act of Hacking, which is illustrative of the general confusion around the nature of Hacking. Hacking is also concerned with status within the community based upon perceived level of skill, which is not the case with the Ethical Hackers who responded to this study who wished to support their colleagues, even if this was only in order to reduce their own workload and therefore selfishly motivated, rather than being for the good of their colleagues, employers or society.

7.4 The Role of Ethics within Ethical Hacking

Not all Ethical Hackers are perceived as being Hackers, and neither are they always Ethical. Ethical Hackers who are drawn from different social backgrounds will follow various different forms of ethical reasoning when they make decisions about how to act while at work, and in their own private time. They do not always use the same reasoning in both, with some indicating that they are deontological in their approach while at work, but consequential, and often hedonistic in their approach while Hacking for leisure. Those who have current affiliations with the Hacking underground, whether they are engaged in actions that are criminal or not, have tended in this research to indicate that they make use of a teleological framework in making decisions about how to behave; they are concerned with the consequences of their actions. Those without these affiliations, and those who are involved in education, either as educators or as students, tended more towards a rule deontology as a mode of reasoning. They act as they would want others within their field to act. They follow parts of the law that they acknowledge to be problematic, because they feel that all of us should follow all of the law.

In chapter 3 a model for understanding Underground Ethical Hacking was proposed based upon three key meta-ethical approaches, in combination with the typologies which are available of Underground Hackers. In chapter six this is developed further in order to show that this also provides a useful framework for understanding the ethical considerations of Ethical Hackers in employment. This is a useful addition to the available typologies, which have limited focus upon the ethical hacker, and which only understand the term Ethical Hacking in the underground, and not the academic sense of the term.

7.5 Ethical Hacking and the Law

Hacking (in relation to unauthorised access) was first criminalized in the UK in 1990 under the provisions of the Computer Misuse Act, which was updated within the provisions of the Police and Justice Act in 2006. Ethical Hackers within this research varied in their perceptions on the current state of the law and also whether and when they chose to adhere to it. It was generally agreed that the law is vague and is ambiguous, and in many cases is problematic for those trying to operate legally. There are particular definitional issues about the nature of computers and networks, and also issues around jurisdiction due to the global nature of Cybercrime as well as concerns that the law is outdated, and that it is currently in need of revision. The revisions to the Computer Misuse Act of 1990 under the Police and Justice Act of 2006 have further criminalized Hacking behaviour by the addition of new offences, and also by increasing the associated penalties. The revisions have also created a situation where Ethical Hackers, researchers or students could inadvertently fall foul of the law during their normal work as the creating of Hacking tools has been criminalized. This is a concern, as it may restrict the future development of the industry if professionals and researchers feel that they are limited in how they operationalise their skills and knowledge. As many do however indicate that they do not always operate within the law, both inside and outside of work, it could be argued that it is necessary to have some protection in law for employers and for individuals. It is hoped that the Criminal Justice System, and in particular the judiciary, will be sensible and fair in how they choose to apply this law so that the development of the field is not restricted in future, and so that the law is applied fairly and appropriately. There are no known cases to date of this legislation being inappropriately used, despite the concerns raised within the industry.

7.6 Ethical Hacking and the Rational Bounded Model

Rational models of behaviour assume that the actor is rational in their decision making processes and that they will weigh up the possible costs and perceived benefits before embarking on a course of action. Bounded models assume that there are boundaries which reduce the rationality of decisions by the inclusion of heuristics, or by the inclusion of emotion and personal circumstances (Simon, 1957; Clarke and Cornish, 1985; Cornish and Clarke, 1986; Gigerenzer and Selton, 2001; Selton, 2001; Cornish and Clarke, 2008). The Ethical Hackers in this study indicated in their responses that they go through these processes when they are making decisions about how they should behave and that norms that they had gained through their socialisation, the law, professional standards and ethical reason acted as heuristics which guided the reasoning process.

Rational models of decision making can be divided into two distinct sections – decisions that are about individual events, and decisions that relate to ongoing criminal involvement. Involvement can be considered under three headings; the decision to begin offending, the decision to continue, and the decision to desist.

7.7 Event decisions

Event decisions are choices that are made about or during the commission of a criminal act. These are based upon the individual's perception of the situation and their assessment of the associated risks and rewards (Clarke and Cornish, 1985; Cornish and Clarke, 1986, Clarke and Cornish, 2000). Event decisions are more likely than long term involvement decisions to be impacted upon by the immediate social setting and situation, and therefore are more bounded, and less likely to produce optimal outcomes (Clarke and Felson, 2008).

Mathematical modelling has indicated that "…a hacker determines whether malicious activity or socially acceptable activities will yield a greater expected utility." (Shim, Allodi, and Massacci, 2012: 4).

It would appear that many of the decisions that are made in the commissioning of actual events are made by weighing up the likely gains and costs. Many of the individual illegal hacking accounts described here would appear to have been rationalised post-fact in line with Sykes and Matza's (1957) suggestion that offenders all rationalise their behaviour. Despite this post event rationalisation it would appear that community, socialisation and prior experience provide the respondents with a set of heuristics. The evidence for this is that different socialisation experiences seem to lead to different behavioural outcomes, despite evidence that the respondents do think through the cost and benefit implications of their actions, both for themselves and for others. Their reasoning process is bounded by the social rules and the personal rules that they have learned in their prior experience and through the agents of their socialisation.

7.8 Involvement

Involvement decisions are choices that an individual makes about their criminal career. The first of these decisions is about whether or not to embark on a criminal career (initiation); following this are decisions regarding whether to stay involved (persistence or habituation, and desistence) (Clarke and Cornish, 2000).

It would appear that many of the respondents embarked on a Hacking career through an initial interest in computers, and that they described this as being common across the field. They begin to engage with the community as a means of advancing their knowledge and their skills, and illicitness and openness are valued in the community, so that illegal activities are not viewed as necessarily being deviant. These community norms can later come to act as heuristics which bound the rationality of later decisions. Those individuals who entered the field in this way are more likely to have embarked on a path of action which involves behaviour that is illegal. Respondents to this study indicated that although it is often a rational course of action to switch from criminal behaviour into legitimate forms of authorised hacking as a career, this is not an option that is open to all; being unemployed will increase the likelihood of continuing in the criminal career (Bachmann, 2010). Despite an awareness of the many benefits of hiring ex-criminals who have chosen to desist, there is a clear reluctance within the industry to employ these individuals who may pose a risk to business, customers, and their colleagues.

The other group of respondents learned to hack later in life, having first worked as policemen, lawyers or in security. These are socialised into very clear ideas about the importance of upholding the law before learning to hack, so choose to act legally in their hacking.

Those with affiliations to the computer underground are more likely to choose to become involved in criminal behaviour, and are more likely to continue. Those with formal education in Ethical Hacking are more likely to reduce their offending, and are more likely to consider and to reduce the harm associated with their offending.

In considering whether to become involved in crime, and whether to continue or desist the respondents indicated that there was a clear process of reasoning involved, whereby the potential costs and gains were calculated. This is not a mathematical calculation, but rather is an approximation of whether certain actions will produce a net gain or a net loss in terms of the inputs and expected outputs. Within this calculation respondents included the level of risk associated, the impact upon their status, reputations and career, the likelihood of prosecution, the level of challenge involved and the level of thrill and excitement provided. These reasoned decisions are bounded by heuristics, satisficing (making do with less than optimal outputs), and by the social and personal contexts of the decision makers and the decisions made.

7.9 Impact of the Research

This research has implications for those individuals and organisations that would employ Ethical Hackers. It is apparent that Ethical Hackers who have no criminal past or affiliations can see clear benefits in employing Hackers who have a criminal or an underground past, as they have the skills, knowledge, and social networks to allow them to be extremely effective in their roles. Those who have engaged in criminality, even where they have been ethical in their decisions, are more cautious; this may be because they have a heightened awareness of the potential risks that are involved, so that when they engage in a cost-benefit analysis they pay more heed to the risks involved . Respondents have indicated that there are issues around lack of trust, the threat to the business reputation and the credibility of the industry, and possible criminality while working. Ethical Hackers seem to lack accountability in that once a system or network has been breached, there are no consequences for them if they further abuse the breach that has already taken place – they are the security experts, and no-one is coming in to check the system after them. This perceived low level of risk or cost increases the likelihood that they will engage in criminality

There are considerations here for both private and public organisations that employ Ethical Hackers, many of whom would avoid hiring those Hackers who have a Criminal record. The respondents to this study indicated that the more skilled Hackers tended to be employed within the private sector, as that is where they could guarantee regular work, a good income, and most importantly for the variety in their work so that they continue to learn and to be challenged; many of these skills were gained from underground activity and affiliations.   Although highly skilled, some self-report that they themselves cannot be trusted not to engage in illegal activity either at work or outside of work. It is notable that where they disregarded the law, or where they were unaware of it that these Ethical Hackers were indeed 'ethical' in their behaviour; generally following a consequentialist utilitarian ethical reasoning, or at least consequentialist hedonism, but with no perceived harm to others. They would engage in criminal behaviour in a fairly rational manner, choosing to break the law only when they saw no harm to others, and when they knew that it was unlikely that they would be caught. They valued their employment and their professional reputations. None of the respondents to this study actually had a criminal record, although it was indicated that a criminal record may be sign of incompetence rather than competence as a hacker, and therefore something to be avoided by the employer when making a hiring decision.

Those Ethical Hackers who stated clearly that they would follow the law, and would follow professional guideline at all times, self-reported that they had lower levels of skills and knowledge than the Hackers who were engaged in criminality and they saw themselves and their colleagues as struggling to keep up with developments in the field, and struggling to cope with the workload that they had. They were generally less passionate about computing, about programming and about Hacking and did not report having had an interest in computing except professionally. They had not entered the field of computer security through an interest or obsession in computing as their counterparts had, rather they had come to computing as a means of doing their job. In this research, these Hackers tended to be employed within the public sector, and they do appear to be very trustworthy, but this may be at the expense of the usually obsessive nature of Hacking, meaning that they are less passionate, less driven, and possibly less skilled and experienced than their counterparts in the private sector and in the computer underground. They may therefore be less effective, but are more appropriate for positions of trust. What is problematic here is that the employer or buyer of the service can have no way of knowing what the level of involvement with the computer underground actually is.

The findings also have relevance for educational professionals who have struggled with the acceptability of selling courses which teach Hacking skills. They are aware that some of what they teach might be used for criminal purposes, but see no way of controlling this, and hope that by educating individuals engaged in the field that they can improve the level of moral reasoning and therefore reduce the likelihood of criminal or harmful behaviours. It would appear that socialisation before entering courses of education had more impact upon offending behaviour, but also that courses of education are also likely to reduce offending behaviour in those who have embarked on criminal careers. There is some evidence that education increases understanding of the impact of actions, and improves moral reasoning so making criminality less likely. It also appears from the evidence here that increasing employability provides an alternative to criminality for many, so that they choose never to engage in criminality, or to desist, or to reduce the amount of offending, or the harm associated with it. As it appears that those who engage in illegal behaviour while employed as Ethical Hackers do so with a very rational and ethical approach, courses of study for Ethical Hackers must contain information about the harms caused by illegal Hacking behaviour, as well as the consequences breaking the law which will minimise any potential harm or criminality. In order to improve moral reasoning it is also important that courses of education should include meta-ethical approaches so that individuals can develop an awareness of their own ethical reasoning, which will also increase their level of moral development. Many of the respondents indicated that they were not familiar with the provisions of the legislation at present, choosing to either see this as their employer's responsibility, or to ignore it altogether and make up their own minds based upon the level of harm that they perceived that they were doing. The law can only act in a normative capacity if people are aware of its provision, so this is an essential part of the Ethical Hackers formal education. Educational professionals may need to consider placing more emphasis on the consequences of illegality for the students and also for their future employers, clients, and potentially any victims of their criminal behaviour. As many Ethical Hackers do not attend courses of study this cannot be solely the responsibility of educational professionals; there is a need also for ongoing training by employers of Ethical Hackers. This still leaves a gap in terms of those Ethical Hackers who are free-lance, and so it may be worth considering some professional accreditation which would include an emphasis on them being able to show an awareness of legislation, penalties and potential harms. Even this ongoing professional requirement will not guarantee desistance, but it appears that it would make it more likely. This would also increase the assurance to the buyers of the service that the Hacker that they are employing is likely to handle their data in a way that is ethical.

Professional standards did not seem to provide a normative function, despite offering a set of uniform standards, or a code of practice to be followed from a recognised professional body. Professional accreditation as an industry requirement could include ensuring that these standards are known, and also that they are updated on a regular basis as is necessary.

7.10 Implications for Further Research

This research relied upon an intensive research design using traditional qualitative methods, within a critical realist analytical framework. This approach was necessary due to the nature of the field of study. As a new area, there were no structures available by which to construct an empirical or large scale study which would be representative and therefore be generalisable to the whole sample frame. This research aimed to present the reality of Ethical hacking through the eyes of a range of key informants in order to tentatively begin to understand a new field of study, and so its aim was to break ground, rather than to be empirical or generalisable. The qualitative approach taken reflects the need for rich in-depth data. The ‘reality’ of the situation of the respondents is in no way reduced by the way in which the data was collected. The typology presented in table 5 within chapter 6 may go some way to providing a framework for further an extensive research project employing quantitative methods that employs larger samples and other research methods in order to find out whether the reality of Ethical hacking that is revealed for the respondents to this study applies elsewhere within the field.

The previous literature and research had mainly focused upon the computer underground, and on practical manuals for Ethical Hackers. The theorising that was already available was found to be only partially applicable to this area of study as it had focused solely upon the application of criminological theory to explain criminality, and did not focus upon why many Hackers chose to 'cross the line' and come to be involved in prevention. Many of the respondents had in fact never been involved with Underground Hacking and make up a distinct group which have not been studied before. This study used a relatively small sample of 23 respondents in order to establish the ground and in order to enable analysis of the extensive data created in narrative style interviewing. Future research will include testing the findings of this research by conducting a larger survey and looking for evidence of correlations which have been suggested, but cannot be conclusively proven here due to the sample size. This will consider the relationships between educational and employment background, socialisation, and behaviour, focusing on whether behaviour is legally sanctioned and whether it can be considered to be ethical under the three meta-ethical approaches discussed. It is also of interest that of the 23 respondents, only one was female. She felt that this affected the way she was perceived, she stated:

> I think I do face a little bit of [pause] erm [pause]. Not prejudice that is too strong a word [pause] but certainly suspicion because I'm female [pause] Nearly all of the people I work with are men, at the same time though I can not help think the novelty of being a woman doing what I do could have helped my career as well as hindering it if in fact it has…. I do think I have had to work harder to prove myself
>
> (Respondent 7)

Gender was outside of the focus of this work, but is clearly an area of further investigation. In Ethical Hacking it would appear that the 'digital divide' is gendered.

This is worthy of further consideration in order to find out whether this is representative of the industry at large, which appears to be male dominated, and if this is the case, then to find out why it is this way. This may require further qualitative research with respondents who come forward who are female, but also with a representative sample of Ethical Hackers in general. It is regrettable that this was not addressed within this research, however, it was not known at the outset that there would be such a marked difficulty in finding any respondents who are female, and therefore was not perceived to be of relevance during the planning stage. This is of interest as computing and programming in general are male dominated, and it is also an accepted fact within sociology that the primary and secondary socialisation of girls is different to that of boys, and that this impacts upon choices that they make in education and in employment.

This research has also only been applicable to the UK, it will be of interest in future to conduct a trans-national analysis, in order to examine whether Ethical Hackers in other legislative jurisdictions share traits with those found in the UK.

Another area which would be of interest for further study would be areas of conflict and competition among Ethical Hackers and also between the industry and the computer underground. This study sought to investigate whether there was a sense of community among Ethical Hackers as has been previously found with Underground Hacking, so the discussion focused around whether there were communication networks, support networks and communication. There has not been a focus upon negative communications and interactions.

7.11 Conclusion

As has been outlined in this Chapter, this PhD thesis has created a new way of understanding Ethical Hacking in relation to ethics and the legislative framework.

There are also new areas of interest indicated for further research and theorising, within Criminology and also within ethical and legal studies. This includes a quantitative analysis of the makeup of the Ethical Hacking community, and a qualitative analysis of the gendered nature of the field.

There are some clear correspondences between Ethical Hacking and Underground Hacking, but also many differences, and a range of clear points of intersection between the two activities and the associated social networks. There are clear implications for a wide range of stakeholders including employers, educational professionals, buyers of the service and those who would seek to regulate and control the industry, which is going through a period of rapid growth. It would appear that it would be a practical step for all Ethical Hackers to go through formal training, which includes the law, professional standards, and philosophical ethics, and to require that they prove this knowledge through professional accreditation. Whilst this produces no guarantees for buyers of the service, it would certainly, according to the findings of this research, reduce criminality, and where it does occur would reduce the associated harms. It is not sufficient to provide regulatory frameworks; there need to be mechanisms which encourage individuals to follow these, because they choose to. The skill level of Hackers means that architectural and other formal controls are not effective.

It would appear that Hacking and Ethical Hacking can be understood as being ‘rational choices’ however these choices are framed, or ‘bounded’ differently for different individuals, therefore producing different outcomes. The implications for the industry are clear:

> System administrators and other IT professionals seeking to reduce security vulnerabilities associated with human factors should seek to incorporate the principles of Rational Choice Theory into their policies, program planning, and management activities… Rational Choice Theory goes to the heart of crime prevention and information security programmes that seek to promote compliance with the existing crime laws, regulations, organizational policies, and procedural rules for using and securing system resources.
>
> (McQuade, 2006: 144)

What this research has revealed is that the rational frameworks employed in decision making among Hackers can be manipulated into reduced offending, or into desistence, by ensuring that there is full awareness of ethical approaches and likely harms by those in the industry, as this knowledge impacts upon the reasoning of the individuals involved. We can not control the Hacker, but we can encourage him to employ ethical and moral reasoning and give him strategies to do so.

> We should have a global hacker appreciation day dedicated to all the hackers, phreakers, crackers, nuts, weirdos, and associated other human beings who surf, spam, use, misuse and abuse the global information infrastructure. Because of their crazy personalities, criminal conduct and all round blatent disregard for rules, laws and government controls, they have kept millions of people employed, made all our lives more interesting, our work more challenging, and our information security market - and world economies - growing!
>
> (Halibozek, Jones and Kovacich, 2007: 208)

This Thesis has explored the nature and practice of ‘Ethical Hacking’. Ethical Hackers are individuals who use hacking skills, knowledge and techniques within legitimate authorised practice; they are employed to Hack.

A Critical Realist methodological approach has been employed in order to gain a qualitative understanding of a real phenomenon through a range of key informants who provide personal narratives within semi-structured interviews, commenting upon their own realities, and their perceptions of the field in which they work.

A Bounded Rational Model of decision making reveals that decisions relating to involvement in criminality and individual Hacking events are made through a process of reasoning, of approximating the net gains and losses of a particular course of action, and that these decisions are 'bounded' by social norms, ethical approaches and the personal motivations and social circumstances within which the decisions and behaviour are framed.

List of References

AOIR (2002) http://aoir.org/2002/ (Accessed: 18 May 2011)

Anderson, B. (1991) *Imagined Communities.* 2nd edn. London: Verso

Anderson, T. B. K. (2001) 'Digital Living: the impact (or otherwise) of the Internet on everyday life*',* *American Behavioral Scientist,* 45(3), pp 456-75

Archer, M. Bhaskar, R. Collier, A. Lawson, T. and Norrie, A. (1998) 'General Introduction, in Archer, M. Bhaskar, R. Collier, A. Lawson, T. and Norrie, A. (eds.) *Critical Realism: Essential Readings*, Routledge, London, pp. ix-xxiv

Arksey, H. and Knight, P. (1999) *Interviewing for social scientists.* London: Sage

Arquilla, J., and Ronfeldt, D. (2001) 'The advent of netwar revisited; Emergence and influence of the Zapatista netwar; What next for networks and netwars?: Afterword (September 2001): The sharpening fight for the future', in Arquilla, J. and Ronsfeldt, D. (eds.) *Networks and netwars: The future of terror, crime, and militancy*. Santa Monica, Arlington and Pittsburgh: RAND.

Athique, A. (2013) *Digital Media and Society- An Introduction.* Cambridge: Polity

Bachmann, M., (2010) 'The risk propensity and rationality of computer hackers' in *International Journal of Cyber Criminology* 4 (1&2): pp 643- 656

Bauer, M. (1996) 'The Narrative Interview: Comments on a technique for qualitative data collection.' *LSE Papers in Social Research*, qualitative series no 1.

Beauchamp, T. and Childress, J.F. (1994) *Principles of Biomedical Ethics.* 4th edn. New York: Oxford University Press

Beauchamp, T. and McCullough, L. (1984) *Medical Ethics.* New York: Prentice Hall

Beck, U. (1992) *Risk Society: Towards a New Modernity.* New Delhi: Sage

Beck, U. (1994) 'The Reinvention of Politics: Towards a Theory of Reflexive Modernization", in Beck, U., Giddens, A. and Lash, S. (eds.), *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order*. Cambridge: Polity Press, pp. 1-55

Bennett, A. (1997). 'Going down the Pub!': The Pub Rock Scene as a Resource for the Consumption of Popular Music', Popular *Music,* 16(1), pp. 97-108

Beniger, J. R. (1986) *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge, MA: Harvard University Press

Benney, M. and Hughes, E.C. (1956) ‘Of Sociology and the Interview’, *American Journal of Sociology,* 62, pp. 137–134

Bentham, J. (1781) ‘An Introduction to the Principles of Morals and Legislation’ [Online] Available at www.utilitarianism.com/jeremy-bentham/index.html (accessed 5th February 12)

Bernard, R. and Ryan, G.W., (2010) *Analyzing Qualitative Data: Systematic Approaches: Systematic Techniques for Collecting and Analyzing Data* London: Sage

Berners-Lee, T. (1996) ‘WWW: Past, Present, and Future’, *IEEE, Computer Magazine*, 29(10), [Online]. Available at: http://www.computer.org/csdl/mags/co/1996/10/rx069-abs.html (Accessed 6th September 2014)

Berners-Lee, T. and Fischetti, M. (1999) *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor.* San Francisco: Harper Collins

Bhaskar, R. (1975) *A Realist Theory of Science*. London: Verso.

Bhaskar, R. and Lawson (1998) ‘Introduction: Basic Texts and Development’ in Archer, M. Bhaskar, R. Collier, A. Lawson, T. and Norrie, A. (eds.) *Critical Realism: Essential Readings*, Routledge, London, pp. 3-15

.Blau, P. M. (1997) ‘On limitations of rational choice theory for sociology’, *The American Sociologist*, 28(2), pp.16-21

Boeije, H. (2010) *Analysis in Qualitative Research.* London: Sage

Boni, W. C. and Kovacich, G. L. (1999) *I-way Robbery: Crime on the Internet.* Woburn: Butterworth-Heinemann

Bowyer, K. W. (2001) *Ethics and computing: living responsibly in a computerized world,* 2nd edn., New York: IEEE

Box, S. (1971) *Deviance, Reality and Society*. London: Cassell

Brenner, S.W. (2004) ‘Cybercrime Metrics: Old Wine, New Bottles?’, *Virginia Journal of Law and Technology,* 9 (4) [Online]. Available at http://www.vjolt.net/vol9/issue4/v9i4_a13-Brenner.pdf (Accessed 6th September, 2014)

Brey, P. (2004) ‘Disclosive Computer Ethics’ in Spinello, R.A. and Tavani, H.T. (eds.) *Readings in Cyber-ethics.* 2nd edn. Sudbury MA: Jones and Bartlett

Broadhurst, R. G. (2006) ‘Content cybercrimes: Criminality and censorship in Asia’, *Indian Journal of Criminology*, 34(1 & 2), pp.11-3

Bryant, R. & Marshall, S. (2008) ‘Criminological and Motivational Perspectives Crime’ in Bryant, R. (ed.) *Investigating Digital Crime.* Chichester: Wiley & Sons, pp. 231-248

Bryman, A. (2008) *Social Research Methods,* 3rd edn. Oxford: Oxford University Press

Buchanan, E. (2004) *Readings in virtual research ethics: issues and controversies.* London: Information science publishing

Byrne, P. (1997) 'Psychiatric stigma: past, passing and to come', *Journal of the Royal Society of Medicine,* 90, pp. 618-621

Capeller, W. (2001) 'Not Such a Neat Net: Some Comments on Virtual Criminality', *Social and Legal Studies,* 10(2), pp. 229-242

Campbell, D. T. (1974) 'Evolutionary Epistemology' In Schlipp, P. A. (ed.) *The philosophy of Karl Popper*. LaSalle, IL: Open Court. pp. 413– 463

Calhoun, C. (1991) 'Indirect relationships and imagined communities: large-scale social integration and the transformation of everyday life', *Social theory for a changing society,* pp. 95-121

Castells, M. (1996) *The Rise of the Network Society.* Cambridge, MA: Blackwell

Cerulo, K. A. (1997) 'Reframing Social Concepts for a Brave New (Virtual) World', *Sociological Inquiry.* 67 (1), pp. 48-58

Chamberlain, J.M. (2013) *Understanding Criminological Research: A Guide to Data Analysis* Sage Publications: London

Chase, S.E. (1995) '*Taking narrative seriously'* In Josselson, R. and Lieblich, A. (eds.) *Interpreting experience: The Narrative Study of Lives*, *Vol 3*. CA: Sage

Cherilla, J. (2002) 'Hackers, Crackers, Phreaks, Script Kiddies and CyberPunks', *Database and Network Journal* (December)

Chiesa, R. and Ducci, S. (no date) *The Hacker Profiling Project* [Online]. Available at http://www.infosectoday.com/Articles/Hackers_Profiling_Project.html (Accessed 28th May 11)

Clarke, R.V. and Cornish, D. (1985) 'Modelling Offenders Decisions: A framework for research and policy' in Tonry, M. and Morris, N. *Crime and Justice: An Annual Review of Research,* vol.6, Chicago: University of Chicago press, pp. 147-85

Clarke, R.V. and Cornish, D. (2000) 'Rational Choice in Explaining Crimes an Criminals' in Paternoster, R and Bachmann, R. *Contemporary Criminological Theory,* CA: Roxbury

Clarke, R. V. and Felson, M. (eds.) (1993). *Routine Activity and Rational Choice. Advances in Criminological Theory*, Vol 5. New Brunswick, NJ: Transaction Books

Cohen, A. K. (1955) *Delinquent Boys: The Culture of the Gang.* NY: Macmillan

Cohen, L. E., & Felson, M. (1979) ‘Social Change and Crime Rate Trends: A Routine Activity Approach’, In *American Sociological Review* 4(4), pp. 588-608

Cornish, D.B., and R.V. Clarke (eds.) (1986). The Reasoning Criminal: Rational Choice Perspectives on Offending. New York: Springer-Verlag

Cornish, D. B., & Clarke, R. V. (2008) ‘The Rational Choice Perspective’, *Environmental criminology and crime analysis,* 21, pp. 21-47

Cornwall, H. (1986) *The new hacker's handbook.* Melbourne: Century Hutchinson Press

Coupland, D. (1995) *Microserfs*. London: HarperCollins

Cresswell, J.W. (2013) *Research Design.* 4th edn. London: Sage

Curran, J. (2010) “Reinterpreting internet history”, In Jewkes, Y. and Yar, M. (eds.) (2010) *The Handbook of Internet Crime.* GB: Willan Publishing

Danermark, B., Ekstrom, M., Jakobsen, L. and Karlsson, J.C. (2002) *Explaining society: critical realism in the social sciences.* New York: Routledge.

Dawson, S. (1986) *Analysing Organisations*. London: Macmillan.

Davies, B. (1993) *The Thought of Thomas Aquinas* Oxford: Oxford University Press

Dalal, A. S. and Sharma, R. (2007) ‘Peeping into a Hacker's Mind: Can Criminological Theories Explain Hacking?’ in *ICFAI Journal of Cyber Law,* 6(4), pp. 34-47

Della Porta, D. and Diani, M. (2006) *Social movements: An introduction.* 2nd edn. Malden, Oxford and Victoria: Blackwell Publishing

Denning, D. E (1990) ‘Concerning Hackers Who Break Into Computer Systems’ In *Proceedings of the 13th National Computer Security Conference,* October 1990, pp.653-664

Denning, D. E. (2001) ‘Activism, hacktivism and cyberterrorism: The internet as a tool for influencing foreign policy’, in Arquilla, J. and Ronsfeldt, D. (eds.) *Networks and Netwars: The future of terror, crime and militancy* : 239-288 Santa Monica, Arlington and Pittsburgh: RAND

Denzin, N.K. (1983) ‘Interpretive Interactionism’ in Morgan, G. (ed.) *Beyond Method: Strategies for Social Research* London: Sage

Denzin, N.K. and Lincoln, Y.S. (2011) *The Sage Handbook of Qualitative Research*. London: Sage

Dibbell, J. (1998) *My Tiny Life: Crime and Passion in a Virtual World.* London: Fourth Estate

Dreyfus, S. (1997) 'Underground: Tales of Hacking, Madness, and Obsession on the Electronic Frontier' [Online]. Available at *http://onlinebooks.library.upenn.edu/webbin/gutbook/lookup?num=4686* (Accessed: 25 May 2011)

Easterbrook, F. (1996) *Cyberspace and the Law of the Horse.* University of Chicago Law Forum 207, pp. 207-2016

Edger-Neville, D. Stephens, P. (2008) 'Countering Cyber Crime', in Bryant, R. (ed.) *Investigating Digital Crime.* GB: Wiley

Elliott, J. (2005) *Using Narrative in Social Research.* GB: Sage

Ess, C. (2006) 'Ethical Pluralism and Global Information Ethics', *Ethics and Information Technology.* 8(4) pp. 215-226

Fadia, A (2005) The Unofficial Guide to Ethical Hacking. 2nd edn. GB: Course Technology Inc.

Fafinski, S., (2009) Computer Misuse: Response, Regulation and the Law. London: Willan Publishing

Ferrell, J. (1992) 'Making Sense of Crime: Review Essay on Jack Katz's Seductions of Crime', *Social Justice,* 19(3), pp.110-123

Ferrell, J. (1997) 'Youth, crime and cultural space', Social Justice. 24, pp. 21-38

Fielding, N. (1981) *The National Front.* London: Routledge

Finch, E. (2001) 'Confidentiality in Research into Criminal Activities; the Legal and Ethical Dilemma', *Mountbatten Journal of Legal Studies,* 34-40

Finnis, J. (1980) *Natural Law and Natural Rights*. New York: Oxford University Press

Finnis, J. (1983) *Fundamentals of Ethics.* Washington DC: Georgetown University Press

Foot, P. (1979) 'Moral Relativism' *Lindley Lecture*, Department of Philosophy, University of Kansas Reprinted in Kraus, M and Meiland, J.W (eds) Relativism: Cognitive and Moral Notre Dame: University of Notre Dame Press pp 152-66

Forester, T., and Morrison, P. (1994) *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing.* Boston: MIT Press

Fotinger, C. S. and Ziegler, W. (2004) Understanding a hacker's mind - A psychological insight into the hijacking of identities. Available on line at: HTTP//www.donau-uni.ac.at/de/starium/fachabte//ungen/tim/zantren/zpi/studentbot/security/danubeuniverstiyhackersstudy.pdf

Foucault, M. (1980). *Power/knowledge: Selected interviews and other writings, 1972-1977*. New York: Pantheon

Furnell S. (2002) *Cybercrime: Vandalizing the information society*. Boston: Addison-Wesley

Gert, B. (1970) *The Moral Rules: A New Rational Foundation for Morality.* New York: Harper and Row

Gert B. (1988) *Morality: A New Justification of the Moral Rules*. Oxford: Oxford University Press

Gert, B. (2004 a) *Common Morality: Deciding What to Do.* Oxford: Oxford University Press

Gert B. (2004 b) 'Common morality and computing' in Spinello, R.A and Tavani H.T, (eds.) *Readings in CyberEthics*. 2^{nd} edn.. Sudbury MA: Jones and Bartlet

Gert B. (2005) *Morality: Its Nature and Justification,* Revised Edition. Oxford: Oxford University Press

Gert, B. (2006) *Bioethics: A Systematic Approach,* 2nd edn. Oxford: Oxford University Press

Gibbs, J.C. (1993) 'Moral-cognitive interventions' In Goldstein, A.P. and Huff, C.R. (eds.) *The Gang Intervention Handbook.* Champaign, IL: Research Press

Gigerenzer,G. and Selten, R. (2001) 'Re-thinking Rationality' in Gigerenzer, G. and Selten, R. (eds.) *Bounded Rationality: The Adaptive Toolbox*. Massachusetts: Dahlem Workshop Reports

Gilboa, N. (1996) 'Elites, lamers, narcs and whores: Exploring the computer underground' in Cherny, L. and Weise, E. (eds.) *Wired_women*. Seattle: Seal Press, pp. 98-113

Giddens, R. (1990) *The Consequences of Modernity.* Cambridge: Polity Press

Giddens, R. (1991) *Modernity and Self-Identity.* Cambridge: Polity Press

Goffman (1968) *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates.* Harmondsworth: Penguin

Gotterbarn, D. (1995) 'Computer Ethics, Responsibility Regained National Forum", *The Phi Beta Kappa Journal*, 71, pp.26-31

Goode, E., and Ben-Yehuda, N. (2010) *Moral panics: The social construction of deviance.* New York: Wiley

Graves, K. (2007) CEH: Official Certified Ethical Hacker Review Guide: Exam 312-50. New York: Sybex/Wiley.

Guba, E.G. and Lincoln, Y.S. (1989) *Fourth Generation Evaluation.* London: Sage

Gubrium, J.F. and Holstein, J.A. (1997) *The New Language of Qualitative Method*. New York: Oxford University Press

Hafner, K. and Lyon, M. (1998) *Where Wizards Stay Up Late: The Origins of the Internet*. New York: Simon and Schuster.

Hafner, K. and Markoff, J. (1991) *Cyberpunk: Outlaws and Hackers on the Computer Frontier.* New York : Simon and Schuster

Halford, S. Savage, M. and Witz, A (1997) *Gender, Careers and Organisation*. London: Macmillan

Halibozek, E., Jones, A. and Kovacich, G.L. (2007) *The Corporate Security Professionals Handbook on Terrorism.* Oxford *:*Butterworth-Heinemann

Hammersley M. and Atkinson P. (2007) *Ethnography: Principles in practice.* Routledge: London

Hampton, K. and Wellman, B. (2003) ‘Neighboring in Netville: How the Internet supports community and social capital in a wired suburb’, *City and Community*, *2*(4), pp. 277-311

Hargittai, E. (2003). ‘The digital divide and what to do about it’, in Jones, D.C. *New Economy Handbook*. San Diego: Academic Press, pp. 821-839.

Hester, D.M. and Ford, P. (2001) *Computers and Ethics in the Cyberage.* New York: Pearson

Himanen, P. (2001) ‘The Hacker Ethic and the Spirit of the Information Age’_UK : Random House, Inc. [Online]. Available at: http://portal.acm.org/citation.cfm?id=558235 (accessed 22nd May 2011)

Hirschi, T. (1969) *Causes of delinquency.* Berkeley California: University of California Press

Hollinger, R. C. (1991) ‘Hackers: Computer heroes or electronic highwaymen?’, *Computers and Society,* 21, pp. 6-17

Holt, T., and Kilger, M. (2008) Techcrafters and Makecrafters: A comparison of two populations of hackers. Charlott, NC: 2008 WOMBAT Workshop on Information Security Threats Date Collection and Sharing WISTDC 08 workshop, pp. 67-78

Holt, T. J., and Schell, B. H. (eds.) (2010). *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. Hersery New York: Information Science Reference

Hope, M. (2010) *Aristotles Ethics, Moral Development and Human Natur*e. London: Continuum

Holstein, J. and Gubrium, J. (1995) *The Active Interview.* London: Sage

Hollway, W. and Jefferson, T. (2000) *Doing Qualitative Research Differently: Free association, narrative and the interview method.* London: Sage

Humphreys, L (1970) *Tearoom trade: impersonal sex in public places.* Chicago: Aldine

Hutchby, I. (2001) ' Technologies, texts and affordances.' In *Sociology*, 35(2), pp. 441-456

Jaishankar, K. (2007) 'Cyber Criminology: Evolving a novel discipline with a new journal', *International Journal of Cyber Criminology,* 1 (1), pp. 1-6

Jewkes, Y. and Yar. M. (2010) 'The Internet, Cybercrime and the Challenges of the 21st Century' in Jewkes, Y. and Yar. M (eds.) *The handbook of internet crime.* GB: Willan Publishing

Johnson, D. R., and Post, D. (1996). 'Law and Borders: The Rise of Law in Cyberspace', *Stanford Law Review*, 48, pp. 136-7

Johnson, D. (1994) *Computer ethics.* 2nd edn. Englewood, N.J.: Prentice-Hall

Jordan, T. (1999) *Cyberpower: The culture and politics of cyberspace and the Internet*. London: Routledge

Jordan, T. (2002) 'Nerdy no more: The culture and politics of cyberspace', *Electronic Journal of Communication,* [Online]. Available at www.cios.org (Accessed 6 September 2014)

Jordan, T. (2008) *Hacking: Digital Media and Technological Determinism* Cambridge: Polity Press

Jordan, T. and Taylor (1998) 'A Sociology of Hackers', *Sociological Review***,** 46 (4), pp. 757 – 780 [Online]. Available at http://www.dvara.net/Hk/1244356.pdf (Accessed 22/5/11*)*

Jordan, T. and Taylor, P.A (2004) *Hacktivism and Cyberwars: Rebels with a Cause*. NY: Psychological press

Kane (1989) *V.I.R.U.S Protection: Vital Information Under Seige*. NY: Bantam

Kant, I. (1959) *Foundations of the Metaphysics of Morals*. Indianapolis: Bobbs Merrill

Kenyon, G.M. and Randall M.L. (1997) *Restorying our lives: Personal growth through Autobiographical Reflection.* Westport, Connecticut: Praeger Publishers

Kiesler, S., Siegel, J. and McGuire, T.W. (1984) 'Social psychological aspects of computer-mediated communication', *American Psychologist,* 39(10), 1123-1134

Kilger, M. (2010) ‘Social dynamics and the future of technology-driven crime’, in Holt T. J. and Schell B. (eds.), *Corporate Hacking and Technology Driven Crime: Social Dynamics and Implications*. Hershey, PA: IGI-Global. pp. 205-227

Kirkpatrick, G. (2004) *Critical Technology: A Social Theory of Personal Computing.* London: Ashgate Publishing

Kohlberg, L. (1976) ‘Moral stages and moralization: The cognitive-developmental approach” in Lickona, T. (ed.) *Moral development and behaviour: Theory, research, and social issues* New York: Holt, Rinehart and Winston, pp.31-53

Kizza, J.M. (2010) *Ethical and social issues in the information age.* 4th edn. London: Springer

Kleespie, S. L. (2000) ‘The Role of ‘White Hat' Hackers', *Information Security* [Online]. Available at: http://www.wbglinks. net/pages/reads/misc/whitehat. html. (Accessed 9th February 2012)

Laub, J. H. and Sampson, R. J. (2003) *Shared Beginnings, Divergent Lives: Delinquent Boys to Age 70.* Cambridge, MA: Harvard University Press

Laurel, B. (1991) *Computers as theatre.* London: Addison Wesley

Law Commission (1989)

Leibrich, J. (1993) *Straight to the Point: Angles on Giving Up Crime*. Otago, New Zealand: University of Otago Press.

Lenk, K. (1997) ‘The challenge of cyberspatial forms of human interaction to territorial governance and policing' in Loader, B.*The Governance of Cyberspace: Politics, Technology and Global Restructuring.* London: Routledge, pp. 126-35.

Lessig, L. (2001) *The Future of Ideas: The Fate of the Commons in a Connected World.* London: Penguin Press

Lessig, L. (1999) *Code, and other laws of Cyberspace*. New York: Basic Books

Lessig L. (2004) *Free Culture: How Big Media Uses Technology and the Law to Lock Down Creativity*. London: Penguin Press

Lessig, L. (2007) *Code V2, and other laws of cyberspace*. New York: Basic Books

Levy, S. (1984) *Hackers: Heroes of the Computer Revolution*. London: Penguin

Levy, S. (2002) *Hackers: heroes of the Computer Revolution*. New edn. New York: Penguin

Lilley, P. (2002a) ‘Who are they and what are they to you?' in *Hacked, Attacked & Abused: Digital Crime Exposed*. London: Kogan Page, pp.40-49

Lilley, P. (2002b) ‘A History of Hacks” In Hacked, and the Myth of Virtual Community’ in Porter, D. (Ed.) *Internet Culture.* London: Routledge ?? check

Lincoln, Y. S. and Guba, E.G. (1985) *Naturalistic Enquiry* London: Sage

Lipton, J.D. (2010) ‘Combating Cyber-victimization’, *Berkeley Technology Law Journal*. 26, pp. 1103-1105

Lockard, J. (1997) *Progressive Politics, Electronic Individualism.* New York: Wiley

Lyng, S. (1990) ‘Edgework: A Social Psychological. Analysis of Voluntary Risk-Taking’, *American Journal of* Sociology, 95(4), pp. 851-886

MacEwan, N. (2008) ‘The Computer Misuse Act 1990: lessons from its past and predictions for its future’, in *Criminal Law Review* (995) [Online]. Available at: http://usir.salford.ac.uk/15815/7/MacEwan_Crim_LR.pdf (Accessed 6th September 2014)

Maner, W. (1996) ‘Unique Ethical Problems in Information Technology’ in Bynum, T. and Rogerson, S. (eds.) *Science and Engineering Ethics (Special Issue: Global Information Ethics),* 2(2) pp. 137-154

Marsh, I. and Keating, M. (2006) *Sociology: Making Sense of Society*. Edinburgh: Pearson

Matza, D. (1964) *Delinquency and Drift.* New York: John Wiley and Sons, Inc.

Matza, D. (1969) *Becoming Deviant.* New Jersey: Prentice-Hall, Inc.

Maxwell, J. A. (2012) *A realist approach for qualitative research*. London: Sage

Meyer, G. (1989) *The Social Organization of the Computer Underground*. Unpublished Master's Thesis, University of Northern Illinois. DE KALB

Meyer, G. and Thomas, J. (1990) ‘The Baudy World of the Byte Bandit: a Postmodernist Interpretation of the Computer Underground’ in Schmalleger, F. (ed.) *Computers in Criminal Justice.* Wyndham Hall: Bristol, Indiana

Prenzler, T. (2009) *Ethics and Accountability in Criminal Justice* Brisbane: Australian Academic Press

McQuade, S.C (2006) *Understanding and Managing Cybercrime.* Boston, MA: Pearson Education

Miles, M.B. and Huberman, M.A. (1994) *Qualitative Data Analysis: An expanded source book*. 2nd edn. London: Sage

Minkes, A.L. (1987) The Entrepreneurial Manager: Decisions, Goals and Business Ideas, Harmondsworth, UK: Penguin

Mishler, E.G. (1986) *Research Interviewing: Context and Narrative Cambridge.* MA: Harvard University Press

Mishler, E.G. (1999) *Storylines: Craft artists' narratives of identity*. Cambridge: Harvard University Press

Mitnick, K. (2003) 'Kevin Mitnick answers' [Online]. Available at: http://slashdot.org/story/03/02/04/2233250/Kevin-Mitnick-Answers (Accessed: 6th September 2014)

Moayedi, B. Z. and Azgomi, M.A (2012) 'A game theoretic framework for evaluation of the impacts of Hackers diversity on security measures', in *Reliability, Engineering and System Safety,* 99, pp. 45-54

Moor, J. H. (1985) 'What is Computer Ethics?' [Online] Available at: http://www.cs.ucdavis.edu/~rogaway/classes/188/spring06/papers/moor.html (Accessed 9th February 2012)

Moor, J.H. (1995) 'What is Computer Ethics?' in Johnson, D.G and Nissen, B. (eds.) *Computers, ethics and social values*. London: Prentice Hall

Moore, G. (2008) 'Re-imagining the morality of management: a modern virtue ethics approach', *Business Ethics Quarterly,* 18(4), pp. 483-511

Mordini, E. (2007) 'Technology and fear: Is wonder the key?', *Trends in biotechnology,* 25(12), pp. 544-546

Mouzelis, N.P. (1967) *Organizations and Bureaucracy: An Analysis of Modern Theories.* London: Routledge and Kegan Paul

Oldenburg, R. (1999) *The Great Good Place: Cafes, Coffee Shops, Community Centers, Beauty Parlors, General Stores, Bars, Hangouts, and How They Get You Through The Day.* New York: Marlowe & Company.

O'Leary, Z. (2004) *The Essential Guide to Doing Research.* London: SAGE

Outhwaite, W. (2007) *New Philosophies of Social Science: Realism, Hermeneutics and Critical Theory.* London: Macmillan Education

Parker, D (1979) *Ethical Conflicts in Computer Science and Technology* (Volume 1). New York: AFIPS Press

Parker, D. B. (1998) *Fighting Computer Crime: A New Framework for Protecting Information*. New York: John Wiley

Parks, M. (1996) 'Making Friends in Cyberspace', *Journal of Communication,* 46 (1), pp. 80-97

Pfleeger, C. (2007) *Reflections on the Insider Threat. Insider Attack and Cyber Security* US: Springer

Pfuhl, E. H. (1987) 'Computer Abuse: Problems of Instrumental Control' *Deviant Behavior,* 8 (2), pp.113-130

Post, J. (1996) The dangerous information systems insider: psychological perspectives. Technical Report, George Washington University, 1998. Retrieved from an archive of http://www.infowar.com. (Accessed 20.02.09)

Purcell, K. (1997) 'Towards a Communication Dialectic: Embedded Technology and the Enhancement of Place', *Sociological Inquiry,* 67 (1), pp. 101-112

Quarterman, J. (1990) *The Matrix: Computer Networks and Conferencing Systems Worldwide*. Bedford: Digital Press

Quittner, J. and Slatalla, M. (1995) *Masters of Deception: The Gang That Ruled Cyberspace*. London: Vintage

Rawls, J. (1971) *A Theory of Justice.* Cambridge: Harvard University Press

Rege, A. (2009) 'Cybercrimes against criminal infrastructures: A study of online criminal organisations and techniques', *Journal of Criminal Justice Studies,* 22(3)

Riessman, C.K. (1993) 'Narrative Analysis', *Qualitative Research Methods Series,* (No. 30). Newbury Park, CA: Sage

Riessman, C. K. (2008). *Narrative methods for the human sciences*. Newbury Park, CA: Sage

Rheingold, H. (1993) *The Virtual Community: Homesteading on the Electronic Frontier.* Menlo Park, CA: Addison-Wesley

Rock, P., (2012) 'Sociological theories of crime' in Maguire, M., Morgan, R., and Reiner, R. (eds.) *The Oxford handbook of criminology*. 5th edn. Oxford University Press

Rosenberg, D. K. (2000) *Open source: the unauthorized white papers*. Hoboken, NJ: John Wiley & Sons.

Rosenblatt, K. S. (1996) *High Technology Crime: Investigating Cases Using Computers.* Cambridge: KSK Publications

Ross, A. (1991) *Strange Weather: Culture, Science and Technology in the Age of Limits.* London: Verso/New Left Books

Ross, W.D. (1930) *The Right and the Good*. Oxford: Oxford University Press

Salus, P. (2008) *The ARPANET Sourcebook: The Unpublished Foundations of the Internet in Peer-to-Peer Communications*, Charlottesville,

Sassi, S. (2005) 'Cultural differentiation of social segregation? Four approaches to the digital divide', *New Media and society,* 7, pp. 684-700

Sayer, A. (2000) *Method in Social Science: A Realist Approach.* 2nd edn. London: Routledge

Sayer, A. (2002) *Realism and social science.* London: Sage.

Schell, B.H. and Martin, C. (2004) *CyberCrime: A reference handbook*. California: ABC-Clio

Schell, B. H., and Melnychuk, J. (2010) ‘Female and Male Hacker Conference Attendees: Their Autism-Spectrum Quotient (AQ) Scores and Self-Reported Adulthood Experiences’, in Holt, T. J. and Schell, B. H. (eds.) *Corporate hacking and technology driven crime: Social dynamics and implications.* Hershey, PA: IGI Global, pp. 144 - 169

Schneier, B. (2003) *Beyond fear: Thinking sensibly about security in an uncertain world* New York: Springer

Schultz, E. (2002) ‘A framework for understanding and predicting insider attacks’, *Computers and Security*, pp. 526-531

Schultz, E. and Shumway, R. (2001) *Incident Response (Landmark)* London: Sams

Seale, C. (1999) ‘Quality in Qualitative Research’, *Journal of Qualitative Enquiry*, 54(4), pp. 465-78

Selton (2001) ‘What is bounded rationality?’ in Gigerenzer, G and Selten, R. (eds.) *Bounded Rationality*: *The Adaptive Toolbox* . Massachusetts: Dahlem Workshop Reports

Sharma, R. (2007) ‘Peeping into a Hackers Mind: Can Criminological Theories Explain Hacking?’ [Online] Available at www.ssrn.com/abstract=1000446 (Accessed 11th Dec 2012

Sharma, V. (2002) *Information Technology Law and Practice* . New Delhi: Universal Law Publishing

Shim, W., Allodi, L., and Massacci, F. (2012) ‘Crime Pays If You Are Just an Average Hacker’, *Science Journal*, 1(2), pp. 44-55

Simon, H. (1957) *Models of man: Social and rational.* New York: Wiley

Simon, H. (1960) *Administrative Behavior,* New York: Macmillan

Simon, H. (1984) ‘Decision-making and organizational design’, in Pugh, D.S. (ed.), *Organization Theory: Selected Readings,* Harmondsworth, UK: Penguin

Skibell, R. (2002) ‘The myth of the computer hacker’, *Information, Communication & Society*, 5(3), pp. 336-356

Soothill, K., Fitzpatrick, C., Francis, B., (2009) *Understanding Criminal Careers.*

Oregon: Willan Publishing

Spinello, R.A. (2011) *Cyberethics: Morality and Law in Cyberspace*. 4th Edition. Sudbury MA: Jones and Bartlet

Spinello, R.A. and Tavani H.T, eds. (2004) *Readings in CyberEthics.* 2nd Edition. Sudbury MA: Jones and Bartlet

Stake, R.E. (1994) ‘Case Studies’ in Denzin, N.K. and Lincoln, Y.S. (eds.) *Handbook of Qualitative Research* CA: Sage

Stamatellos, G. (2007 and 2011) *Computer Ethics: A Global Perspective.* London: Jones and Bartlett

Sterling, B. (1992) *The Hacker Crackdown: Law and Disorder on the Electronic Frontier.* New York: Bantam Books

Stewart, C., Smith, C., and Denton, R. E. (1984) *Persuasion and Social Movements*. Waveland Press: Prospect Heights, Illinois

Stouffer, K., Falco, J. Scarfone, K. (2011) ‘NIST Guide to Industrial control Systems (ICS) Security’ [Online] Available at http://www.csrc.nist.gov/publications/nistpubs/800-82/sp800-82.final.pdf (Accessed 21st Dec 2012)

Strauss, A. and Corbin, J.M. (2007) *Basics of Qualitative Research*: *Techniques and Procedures for Developing Grounded Theory*. London: Sage

Sykes, G. and Matza, D. (1957) ‘Techniques of Neutralization: A Theory of Delinquency’, *American Sociological Review,* 22(6), pp. 664-670

Sveningsson, M. (2003) ‘Ethics in Internet Ethnography’ in Buchanan, E.A. (ed.), *Virtual Research Ethics: Issues and Controversies*. Hershey, PA: Idea Group Publishing

Tapper, C. (1987) ‘Computer Crime: Scotch Mist?’ in *Criminal Law Review.* 5

Taylor, P.A. (2000) ‘Hackers: Cyberpunks or Microserfs?’, in Loader, B. (ed.) *Cybercrime*. London: Routledge

Tavani, H.T. (2004) *Ethics and Technology: Issues in an age of communication technology* NJ: Wiley

Tavani, H.T. (2007) ‘Philosophical Theories of Privacy: Implications for and Adequate online privacy policy’, *Metaphilosophy,* 38(1), pp. 1-22

Tavani, H.T. (2011) *Ethics and Technology: Controversies, Questions and Strategies for Ethical Computing.* 3rd edn. US: John Wiley

Toby, J. (1957) ‘Social Disorganization and stake in conformity complimentary factors in the predatory behaviour of hoodlums’, in *Journal of Criminal Law, Criminology and*

Police Service 48, pp.12-17

Thomas, D. (2002) *Hacker Culture.* Minneapolis: University of Minnesota Press

Thompson, (1997)

Turkle, S. (1984) *The Second Self: Computers and the Human Spirit.* Simon and Schuster: New York

Turkle, S. (1995) *Life on the Screen: Identity in the age of the internet.* New York: Simon and Schuster

Thompson (1997) 'Center for International Education, U. S. Department of Education: The evolution of sociolinguistics', In Paulston, C. B. and Tucker, G. R. (eds.), *The early days of sociolinguistics: Memories and reflections.* Dallas: Summer Institute of Linguistics

Van Houweling, D and Hanss, T. (2005) 'Internet2: The Promise of Truly Advanced Broadband', in Austin, R. and Bradley, S. (eds). *The Broadband Explosion.* Cambridge, MA: Harvard Business School Press

Venkatesh, S. (1989) *Gang Leader for a Day*. NY: Penguin

Walden, I. (2011) 'Computer Crime and Information Misuse', in Reed, C. and Angel, J. (eds.) *Computer Law,* 7th edn. Oxford: Oxford University Press

Wall, D. S. (2010) 'Criminalising cyberspace: the rise of the internet as a "crime problem"' In Jewkes, Y. and Yar, M. (eds.) (2010) *The handbook of internet crime*. GB: Willan Publishing

Wall, D. S. (2001) 'Cybercrimes and the internet', in Wall, D. (ed.) *Crime and the internet.* London: Routledge

Wall, D. S. (2007) *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity

Walters, R. *(*2003*)* Deviant *Knowledge –Criminology, Politics and Policy*. Devon: Willan Publishing

Ward, K.J. (1999) 'Cyber-ethnography and the emergence of the virtually new community', *Journal of Information Technology*, 14(1), pp. 95-105

Wark, M. (2004) A *Hacker Manifesto*. Cambridge, MA: Harvard University Press

Wasik, M. (2008) 'Computer misuse and misconduct in public office', *International Review of Law Computers & Technology,* 22(1-2), pp. 135-143

Weber, S. (2003) *The Internet.* NY: Chelsea House Publishing

Wenger, E. (1998) *Communities of Practice - Learning, Meaning, and Identity.*

New York: Cambridge University Press.

Weis, L., and Fine, M. (2000) *Speed Bumps: A Student-Friendly Guide to Qualitative Research*. Williston: Teachers College Press

Fine, M. and Weis, L (2003) *Silenced Voices and Extraordinary Conversations: Re-imagining Schools* Williston: Teachers College Press

Wellman, B. (1999) 'The network community' in Wellman, B. (ed.), *Networks in the Global Village.* Boulder, CO: Westview, pp. 1-48

Wessells, M. (1990) *Computer, Self and Society.* Englewood Cliffs, NJ :Prentice Hall

Weiss, R. S. (1994) *Learning from Strangers: The Art and Method of Qualitative Interview Studies*. New York: Free Press.

Williams, M. (2006) *Virtually Criminal: Crime, Deviance and Regulation Online.* London: Routledge

Winner, L. (1997) *'*Technology today*:* Utopia or Dystopia*?'* , *Social Research* 64, pp. 985-1017

Willis (1977) *Learning to Labour: How working class boys get working class jobs.* Farnborough: Gower Publishing

Whyte, W. F. (1955) *Street Corner Society: The Social Structure of an Italian Slum*. Chicago: University of Chicago Press.

Yar, M. (2005) 'Computer Hacking: Just another case of juvenile delinquency?', *The Howard Journal*, 44 (4), pp. 378-399

Yar, M. (2006) *Cybercrime and Society.* London: Sage

Statutes

Great Britain. Computer Misuse Act 1990 (Amendment) Bill 2002: Elizabeth II London: The Stationary Office.

Great Britain. The Computer Misuse Act 1990: Elizabeth II (1990) London: The Stationary Office.

Great Britain. The Criminal Justice and Public Order Act 1994: Elizabeth II (1994) London: The Stationary Office.

Great Britain. The Forgery and Counterfeiting Act 1981: Elizabeth II Section 1 (1981) London: The Stationary Office.

Great Britain The Police and Justice Act 2006: Elizabeth II (2006) London: The Stationary Office.

Great Britain. The Protection of Children Act of 1978: Elizabeth II (1978) London: The Stationary Office.

Great Britain. The Theft Act 1968: Elizabeth II. Section 1. (1968) London: The Stationary Office.

Great Britain. House of Commons, All Party Internet Group (2004) Revision of the Computer Misuse Act": Report of an Inquiry by the All Party Internet Group London: Stationary Office Available at http://www.apcomms.org.uk/apig/archive/activities-2004/computer-misuse-inquiry/CMAReportFinalVersion1.pd