

# **Peeping Into A Hacker's Mind: Can Criminological Theories Explain Hacking?**

## **I. INTRODUCTION**

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

-Sun Tzu, Chapter III, The Art of War

Sun Tzu's exposition about knowing one's enemy has emerged as a recondite problem for legal scholars in the face of lack of efficient rules concerning hacking and continues to haunt them due to lack of understanding of the operating criminal mind and its underlying designs and motivations. The information revolution has led to creation of 'information highways' operating across the globe through interconnected computer networks. The change has been unprecedented but surely not without pitfalls. The rapid metamorphosis of social values and structures is resulting into a control deficit and the consequent emergence of new computer crimes like hacking which have transgressed national boundaries through a burgeoning interconnected cyberspace (which has amplified opportunities for crimes like privacy violation and the information theft). Given the presence of the networked computers in almost every aspect of modern life, the amount of sensitive information stored on networks, and the relative ease with which computer crimes may be committed, the study of computer crime demands greater attention from researchers, law enforcement agencies and legislators. Law codes throughout the world have proved ineffective in curbing the expanding domain of hacking behaviour and hence a need has arisen to re-look at the strategies for containing this emergent menace. This paper seeks to make a modest attempt to peep into the hacker's mind i.e. to understand the criminal behaviour of hackers and locate the source of the rot. I seek to deploy the traditional criminological theories based on psychology, social learning and rational choice to examine how they may be applied to develop an

understanding of this new deviant behaviour. However, this paper is only a modest attempt to understand the explanations that these theories may provide for hacking and thus does not seek to delve into the empirical verifications and other abstract theoretical or logical contradictions that have been offered by the critics.

## II. “HACKER”: THE CLASSICAL CONUNDRUM OF CLASSIFICATION

In order to explore the working of the criminal mind, it is required to develop an understanding of different hacking-types so that there can be systematic deduction and analysis of behavioural differences with varied underlying motivations. Rogers (2002) argues that hackers are not a homogenous group and granulization and classification is essential to pin up researches on understanding their behaviour. Generally speaking, hacking is a successful or unsuccessful attempt to gain unauthorized use or unauthorized access to a computer system.<sup>1</sup> However, a lack of consensus over the connotation of the term ‘hacker’ has been evident over the years. Originally, the term denoted outstanding and radical programmers in the computer science fields who hailed usually from Berkley, Stanford or MIT.<sup>2</sup> Later, the concept underwent radical metamorphosis. Hollinger (1988), based on a progression ranging from less skilled to technically elite computer crimes, divided hackers into three categories: *pirates*, *browsers*, and *crackers*. Pirates, the least technically proficient hackers, confine their activities to copyright violations through software piracy. The browsers, with a moderate technical ability, gain unauthorized access to other people’s files but do not usually damage or copy the files. The crackers, the most proficient hackers, abuse their technical abilities by copying files or damaging programs and systems. McAfee Corporation adopts the classification of hackers into *White Hats* and *Black Hats*.<sup>3</sup> White Hats tend to find flaws in security networks for security corporations and thus contribute to the beneficial improvement of computer

---

<sup>1</sup> Under Section 66 of the Information Technology Act, 2002, a person is said to have committed hacking if he, with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means.

<sup>2</sup> Peter T. Leeson & Christopher J. Coyne, *The Economics Of Computer Hacking*, 1 J.L. Econ. & Pol’y 511 (2005), at 513.

<sup>3</sup> See Cynthia Fitch, *Crime and Punishment: The Psychology of Hacking in New Millenium*, (Dec 16, 2003), retrieved from <[http://www.giac.org/practical/GSEC/Cynthia\\_Fitch\\_GSEC.pdf](http://www.giac.org/practical/GSEC/Cynthia_Fitch_GSEC.pdf)> (Last accessed on July 10, 2007).

services for the users. Black Hats, the ill-intentioned hackers who abuse their skills, can be further subdivided into *angry hackers*, *script kiddies*, and *agenda hackers*. Angry hackers, motivated by hatred for a particular company or group, dedicate their resources to harm them. Script kiddies create mischief on the internet for fun and use hacking tools made by others. Agenda hackers include those disillusioned by political or economic agendas or engaging in terrorist activities through large scale disruption of computer networks. Lemos (2002) refers to a third group of hackers called *Gray Hats* who are independent security experts, consultants or corporate security researchers and are essentially reformed Black Hats like Kevin Mitnick.<sup>4</sup> Finally, Rogers (2002), using the findings from works of the computer security industry has categorized hackers into seven distinct groups on a continuum of lowest to highest technical ability<sup>5</sup> viz. *Tool kit/Newbies* (NT), *cyberpunks* (CP), *internals* (IT), *coders* (CD), *old guard hackers* (OG), *professional criminals* (PC) and *cyber-terrorists* (CT). The NTs are at initial stages of hacking with limited programming skills and use tools and information provided on internet by experienced hackers. CPs, skilled enough to write their own programs, maliciously deface web pages and send viruses, worms and junk mails. Disgruntled employees or ex-employees who hack into or attack their employer's computer systems either by abusing their privileges or special knowledge constitute the internal group and conduct a formidable 70% of all hacking activity. OG hackers have high levels of skill and understanding of computer systems and programming but are not malicious in their intent and look upon hacking as an intellectual endeavour. Lastly, the PCs and CTs, the most dangerous hackers, are highly skilled, use the latest technology and may act as mercenaries for corporate or political purposes.

### III. A PSYCHODYNAMIC PERSPECTIVE ON HACKING

Psychodynamic theories of crime were built on the ashes of Cesare Lombroso's famous biological theory of crime which had conjured up a 'predestined actor model' for the

---

<sup>4</sup> Mitnick had been convicted for a four year term for his hacking spree in US and is presently acting as a security advisor forming his own security company. He is being hired by companies to break into their computer networks, reveal their security system weaknesses, and teach them how to better protect themselves at high pay packages. See Talya Halkin, *Legendary hacker Mitnick turns legit*, The Jerusalem Post (Feb. 24, 2006).

<sup>5</sup> See also Cynthia Fitch, *supra* note 3.

criminal and explained criminal activity as an outcome of factors internal to human body creating inherent 'criminal dispositions'. They brought forth the 'criminal mind' as the force behind crime, operating free from differences of social milieu.<sup>6</sup> There seems to be a natural link between hacking activities and hacker's psychology as they indicate premeditated and learnt patterns of behaviour. I propose to discuss three prominent psychological theories viz. Sigmund Freud's psychoanalytic theory, B.F. Skinner's Operant Conditioning and Hans Eysenck's EPN theory.

#### **(A) The New Age Hacker & Freud's Psychoanalysis**

Psychoanalytic theory, as developed by Sigmund Freud, relies on the hypothetical fragmentation of human personality into unconscious and conscious forces.<sup>7</sup> Freud proposed that human conduct is governed by three forces viz. Id, Ego and Superego. Id represents the unconscious impulsive force which includes primitive biological needs like thirst, hunger and sex etc. He proposed a conflict of Id with Superego, which according to him, represented the inner moral agency, whose development depends primarily on satisfying parent-child relationships. The formation of superego depends on the norms and moral values learnt by the child from his parents and guardians. In this paradigm, ego represents the conscious part of personality which seeks to balance the above two opposing forces. Behaviour depends on the balance of the psychic energy system and any disturbance in this system may produce maladaptive development.<sup>8</sup> Thus, he highlighted two causes of deviant behaviour (1) an inadequate superego formation and functioning due to impaired parent-infant relationships whereby the individual fails to control the impulse of Id, and (2) repressed unconscious desires stemming from a failure to express strong emotional ties with another person, often the parent. August Aichhorn, another renowned psychoanalyst, stated that there was some underlying predisposition termed "latent delinquency" which causes the later criminal behaviour. A failure in psychological development accentuates the initial asocial tendency (latent delinquency) with which every child is born and thus results in deviant behaviour. Other

---

<sup>6</sup> See Roger Hopkins Burke, *An Introduction to Criminological Theory* (Lawman Pvt. Ltd., New Delhi, 2001) p. 77.

<sup>7</sup> See Larry J. Seigel, *Criminology* (Wadsworth, 7<sup>th</sup> ed., 2000) p.163.

<sup>8</sup> Burke, *supra* note 6, at pp.78-79.

psychoanalytic theorists felt that the inability to postpone immediate gratification in order to achieve greater long-term gains was a key factor in criminal behaviour.<sup>9</sup>

Strictly, psychoanalytic theories are more suited for crimes that result from unconscious conflicts like sexual offences or kleptomania. They are not well equipped to explain pre-meditated and planned computer crimes. The psychoanalytic theories concentrate mainly on unconscious factors and the child-parent interactions. A failed bond with a parent is unlikely to lead a child to acquire computer knowledge and practice hacking. Rogers (2000) argues that although several of the more infamous hackers had associations with dysfunctional families, this is not sufficient to explain their choice of the criminal activity to engage in as hacking does not seem to fit in the traditional view of “repressed desires” in the unconscious. Hacking is a conscious activity dependent on specific technical skills, operational knowledge of computers, networks and advanced technological understanding. To be successful at hacking the individual also has to plan the attack in some detail i.e. choose victim system or networks based on their security levels or other interests of the hacker. Thus, Freudian psychoanalytical theory fails to account for the emergent hacking behaviour due to its inherent structural constraints.

### **(B) Is Hacking a Conditioned Behaviour?**

B.F. Skinner’s has argued that human behaviour is determined by the environmental consequences it produces for the individual involved. A behaviour that produces beneficial and desirable consequences multiplies in frequency; which is called *reinforcement* of the said behaviour. On the other hand, behaviour, which produces undesirable consequences, decreases in frequency due to *punishment*. Behaviour therefore operates on the environment to produce results that are either reinforcing or punishing.<sup>10</sup> Thus, a rewarding criminal activity leading to increase in prestige, money, or feelings of adequacy makes the person more likely to engage in further criminal activity. If the consequences are negative viz. arrest or ostracisation, then the frequency of future criminal behaviour should be reduced. Operant conditioning can be used to explain general delinquency as opposed to focusing on specific offences where its application is structurally constrained due to uncertainty in determination of offence-specific levels of

---

<sup>9</sup> *Id*, at p.79.

<sup>10</sup> *Id*, at pp.83-84.

rewards and punishments. Penalties for computer crime may have minimal effect as hackers constitute a counterculture and operate in a world of anonymity where chances of being caught are miniscule. In such a scenario, penalties might serve more as a challenge to boast about eluding them. Wible (2003) also argues that punishment alone may not be the best preference-shaping model in the computer-crime context. Moreover, hackers who have been caught and repeatedly punished, with no obvious reinforcement, still continue to engage in the activity as if it was an ‘addiction’.

### **(C) Hans Eysenck’s Theory: The EPN Criteria**

Focussing on influence of both social and biological factors on individual personality, this theory is based on the notion that through heredity some individuals are born with certain learning abilities which are conditioned by environmental stimuli. The theory is premised on two dimensions of personality viz. extraversion (E) and neuroticism (N) existing on a continuum. The extraversion dimension ranges from high (extravert) to low (intravert) and neuroticism dimension from high (neurotic) to low (stable). There is a separate third dimension called ‘psychoticism’ (P) which seeks to measure attributes such as aggression, preference for solitude, and lack of feelings for others.<sup>11</sup> According to the theory, children learn to control antisocial behaviour through the development of a conscience which is a set of conditioned emotional responses to environmental stimuli associated with antisocial behaviour e.g. an act of punishment from a parent for some antisocial act. The conditioning socializes the child but its nature is integrally connected with the EPN parameters of an individual’s personality. High E and high N scores indicate poor conditionability and poor socialization producing an inclination towards criminal behaviour. On the other hand, low E and low N scores lead to good conditionability and effective socialization resulting in better internalisation of social norms and reduced deviancy. High scores on the third dimension psychoticism (P) would indicate hostility towards others and an inclination to more aggressive, violent criminal behaviour.

---

<sup>11</sup> *Id.*, at pp. 84-85.

Rogers (2000) points out that Eysenck's theory is "geared more toward anti-social behaviour, and has had mixed results in predicting general deviancy". The development of conscience in relation to hacking activity becomes irrelevant as parents are unaware of basics of computers and thus fail to condition the children in the right direction. There are hardly any crystallised social norms or morals governing use of the new computer technology. Thus, the proposition that a conditioned moral reflex against hacking can develop in such a state of absolute moral ambiguity is untenable. Moreover, the theory would predict that hackers should be high on the extraversion scale i.e. having unstable personalities. However, Rogers (2000) argues that the majority of the arrested hackers and those, which have responded to surveys, indicate they are withdrawn, uncomfortable with other people and are *intraverts*. The theory fails on certain major behavioural explanations concerning hackers' personalities.

#### **IV. I HAVE LEARNT TO HACK: APPLYING SOCIAL LEARNING THEORIES**

Social learning, as Seigel (2000) puts it, looks upon crime as a product of learning the 'norms, values and behaviours' associated with the criminal activity. This may involve the acquisition of knowledge concerning the techniques of crime commission and achieving moral disengagement by discovering appropriate rational justifications for the deviant behaviour. *Prima facie*, hacking appears to be a learnt and acquired behaviour and thus it becomes a moot question: how the hacker learns to hack? Learning theories may help in discovering the agencies and social processes (based on interaction through the internet) through which a predilection for hacking and the knowledge to implement it may be acquired. In this respect, I propose to examine the Differential Association theory proposed by Sutherland, the Differential Reinforcement theory propounded by Ronald Akers and the Neutralization theory of David Matza and Gresham Sykes.

##### **(A) Differential Association and Differential Reinforcement**

The explanation of hacking through social learning theory approach is inextricably linked to one of the core sociological theories of crime i.e. Sutherland's differential association theory. Differential association is premised on the notion that modern society contains conflicting structures of norms and behaviours giving rise to crime which is a learnt

behaviour. Normative conflict at the individual level is translated into individual acts of delinquency through differential association learnt through communication usually in intimate groups. In other words peer pressure and peer attitudes influence behaviour.<sup>12</sup> Contact with persons who have favourable definitions towards crime, leads to an individual learning similar definitions. The theory does not indicate that the group of association has to be one of criminals; rather the group should express favourable attitudes toward crime. When criminal behaviour is learnt, the learning includes techniques of committing the crime, which are sometimes very complicated, sometimes simple and the specific direction of motives, drives, rationalizations, and attitudes. When the criminal contacts outweigh the non-criminal contacts of a person depending on the frequency, duration, priority, and intensity, he resorts to crime. Ronald Aker's theory of Differential Reinforcement stems from Sutherland's idea that learning is a component of criminal behaviour and Skinner's theory of operant conditioning. The theory agrees that criminal behaviour is learnt through the various groups and associations which an individual maintains. It goes further to state that the behaviour then continues or is maintained directly by the consequences of the act i.e. operant conditioning. It states that a criminal act occurs in an environment if the individual has been reinforced for behaving in a similar fashion in the past, and the negative consequences of the behaviour are very weak to produce deterrence. However, the learning becomes complex due to differential schedules of reinforcement and punishment involved in a criminal activity. This may result in crystallisation of such deviancy into a personality trait or habit.<sup>13</sup> The use of differential reinforcement theory has been historically focussed on stealing and property related offences as they fit nicely into the theory due to assured positive gains unless the individual is arrested.

Sutherland's theory easily applies to hacking as a person learns hacking through online communities which share such information. However, after the simple learning process is over Aker's theory comes into play in a big way to help the individual maintain his deviancy. It is evident that the hackers are learning their respective criminal behaviour,

---

<sup>12</sup> Sutherland & Cressey, *Principles of Criminology* (Times of India Press, Bombay, 6<sup>th</sup> edn., 1968) pp.75-80.

<sup>13</sup> See Burke, *supra* note 6, pp. 93-94.



and are doing so amongst individuals who hold positive attitudes toward such behaviour. The continuation of hacking may be due to several reinforcing factors viz. increase in knowledge, prestige within the hacking community or overall fame by focussed media attention.<sup>14</sup> In some rare cases, prestigious companies have hired hackers who have penetrated their systems e.g. the legendary Kevin Mitnick which has created an impression that hackers can acquire good jobs in the computer security industry. Rogers (2002) gives an example of an Israeli youth charged with attacking US Military networks who was given a lucrative promotional contract with a European computer manufacturer, and was praised by the Prime Minister of Israel for his ingenuity. He illustrates the serious undermining of punitive elements in anti-hacking laws by the lack of stiff sentences e.g. in Canada, the average sentence for the offence is an alternative measures for a youth and a conditional discharge for an adult.

The core concepts of differential reinforcement, learned behaviour through various groups, and maintenance of the behaviour via reinforcement appear to be especially relevant to hacking. Adamski (1999) has pointed out the existence of popular hacker cultures and sub cultures through data gathered on internet search engines across 14 countries. Although hackers are thought to be solitary with less developed social skills, social skills, they still have an empirically proved desire for affiliation and recognition by peers. Hackers tend to associate with other individuals who also engage in hacking behaviour in the form of purely electronic associations e.g. online chat sessions, or more intimately through hacking clubs like Cult of the Dead Cow CDC, Legion of Doom etc. Adamski (1999) points out how hackers even hold conventions such as the Defcon in Las Vegas to share their skills, ideas and technical information. Thus, both Sutherland's and Aker's theories provide a highly useful insight to the dynamics behind hacking activities.

### **(B) Albert Bandura's Social Learning Theory**

Albert Bandura's social learning theory states that both deviant and normative human behaviour is learned through a mix of observed behaviour, communication with others,

---

<sup>14</sup> See Peter T. Leeson & Christopher J. Coyne, *supra* note 2, at 524, report that hackers may generate instant 'stardom' through participation and peer recognition in online communities.

encounters with disciplinary action and cognitive modelling.<sup>15</sup> The learning at cognitive level occurs in the family, subcultures and the social environment through observation whereby people imagine themselves in similar situations with similar outcomes. The learnt behaviour may be reinforced or punished. In this respect, Bandura subscribes to several essential concepts of the operant conditioning theory viz. reinforcement, punishment, and motivation. He enumerates three aspects to motivation viz. external reinforcement, vicarious reinforcement, and self-reinforcement. External reinforcement is similar to Skinner's concept of reinforcement. Vicarious reinforcement is derived from observing other people's behaviour being either reinforced or punished. Self-reinforcement refers to one's sense of pride or self image or self expected standards of behaviour. Criminal behaviour is maintained through a complex schedule of reinforcement and punishment throughout the life of the individual. If criminal behaviour has been reinforced in the past, there is expectancy that it will be reinforced in the future. The theory has primarily been used to understand aggressive behaviour and violent criminal offences such as assaults or robbery.<sup>16</sup>

This theory can be successfully used to understand the behaviour of hacking. The theory states that criminal behaviour is acquired through observational learning, and the reinforcement from the behaviour comes from external and internal sources. As previously stated, hacking is a behaviour where imitation and modelling seem to play an important role. It has been likened to a subculture, which reinforces adherence to its own moral code. In case of computer activity, the peer group or social circles which influence the deviant behaviour of hackers are virtual. Hacking is a matter of expertise as it involves knowledge of inter-connected cyber information highways and their functioning which cannot be within the exclusive domain of anyone individual. The new age computer culture has changed the nature of physical association and interaction to cyber-interaction which is not limited by boundaries of physical locations. Thus, hackers learn and improve their skills through exchange of information mainly on the Internet Relay Chats and special forums. Cynthia Fitch (2003) points out that the lengthy existence of

---

<sup>15</sup> Alfred L. Mcalister & Albert Bandura, *Mechanisms Of Moral Disengagement In Support Of Military Force: The Impact Of Sept. 11* , Journal Of Social And Clinical Psychology, Vol. 25, No. 2, 2006, p.141, at 142-147.

<sup>16</sup> *Ibid.*

hacker groups like cDc (Cult of the Dead Cow) and L0ph for many decades and closely knit work culture points out to a more personal relation between elite hackers. The existence of hacker subcultures justifies the application of social learning theory. Bandura's social learning constructs have also been successfully applied to music piracy through peer-to-peer networks.<sup>17</sup>

### **(C) Neutralization Theory & Hacking**

David Matza's and Gresham Sykes's Neutralization Theory regards process of becoming criminal as a learning experience.<sup>18</sup> They argue that all criminals have conventional values and attitudes like normal people but what distinguishes them is their uncanny ability to drift from the normal life to existing parallel subterranean values<sup>19</sup> through certain neutralization techniques like denial of responsibility, denial of injury and denial of victim.<sup>20</sup> This helps criminals to cleanse their moral conscience and remove the feeling of guilt. Spafford (1990) lists three major ethical justifications for hacking as improvement in security by discovering loopholes, knowledge acquisition by students and protection of society against corporations by ensuring free access to information. The peer groups contribute in such moral disengagement by lavishing praise on the hacking exploits of individuals and creating an impression that the activities are justified. Rogers (2001) has reported that:

“Self censure can be disengaged or weakened by stripping the victim of human attributes, or shifting the blame onto the victim...Blaming the victim or circumstances allows the perpetrators to view themselves as victims who were provoked. The perpetrator's actions now become

---

<sup>17</sup> Nathan W. Fisk, *Social Learning Theory as a Model for Illegitimate Peer-to-Peer Use and the Effects of Implementing a Legal Music Downloading Service on Peer-to-Peer Music Piracy*, A Thesis Presented to The Faculty of the Department of Communication (September 14, 2006), retrieved from <<https://ritdml.rit.edu/dspace/bitstream/1850/2737/1/NFiskThesis09-14-2006.pdf>> (Last accessed on July 10, 2007).

<sup>18</sup> See Seigel, *supra* note 7, at p.232.

<sup>19</sup> Matza and Sykes define 'subterranean values' as the morally tinged influences that have become entrenched in the culture and are privately practiced and admired but are publicly condemned.

<sup>20</sup> Matza and Sykes offer five such techniques (viz. condemnation of the condemned and appeal to higher loyalties) out of which only three may correctly apply to hacking behaviour.

construed as defensive. The victims are blamed and accused of bringing the actions upon themselves.”<sup>21</sup>

Hackers often blame the system administrator for improperly securing his system or for denying access to sites that they legitimately think they should be allowed to access e.g. university’s system administrator denying access to movie download sites is used as a pretext to hack the administrator as low cost entertainment is considered as an essential ingredient of student life by the hackers. Hackers also blame software vendors for restricting access to free flow of information and thus morally justify their activity as being conducive to ensure information to everyone acting as self proclaimed knight-errants. This behaviour reflects the popular ‘Robin Hood’ syndrome by which individuals neutralize their ethical judgments.<sup>22</sup> Hacking sub-cultures entrenched on the internet offer examples of the parallel subterranean culture which appreciates the publicly illegal hacking activities. Thus, it is safe to conclude that Matza’s and Sykes’s Neutralization theory succeeds in explaining hacker behaviour to a certain extent.

## **V. HACKING & COGNITIVE THEORIES**

Cognitive theories, though a subset of psychological theories, have a basis different from psychodynamic theories. They focus on the dynamics of mental process and the cognitive schemes through which people perceive and represent the world. In this section, I propose to utilise the major theory falling in the moral development branch viz. Kohlberg’s Moral Development Theory.

### **Kohlberg’s Moral Development Theory**

Grounded in the belief of an indispensable link between social and moral development, Kohlberg’s theory of moral development postulates that moral reasoning develops in a sequential manner as the person matures. Broadly, Kohlberg divides the moral development of a person into three stages. The lowest stage is called the *preconventional stage* which typifies criminals i.e. stage where people put their desires first and obey law

---

<sup>21</sup> Marcus Rogers, *A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study* (2001), University of Manitoba, Canada, p.40.

<sup>22</sup> See Susan J. Harrington, *Software Piracy: Are Robin Hood & Responsibility Denial at Work?*, cited from Ali Salehnia, *Ethical Issues of Information Systems* (IRM Press, Hershey, USA, 2002) p.179.

only for the fear of punishment. Beyond this lies the *convention stage* where people learn to obey law and accept it from the viewpoint that it ought to be followed and finally the *post conventional stage* of a fully morally developed character where individual can test the law against abstract concepts such as justice, fairness and respect for human beings and their rights. Criminal behaviour arises when an opportunity to offend occurs and there is a delay in the development of moral reasoning in the individual. The individual cannot control the temptation to engage in the activity and commits the crime. Siegel argues that the structural constraints of the theory limit its application to understanding of general delinquency and possibly white-collar and corporate crime.<sup>23</sup> Rogers (2001) proposes that moral development theory is useful only in understanding a subset of hackers. He points out that documented anecdotal accounts of the lack of concern by hackers over the systems they have attacked and written interviews with convicted hackers portray them as being more concerned with fulfilling their own material needs regardless of the consequences and Kohlberg's lower pre-morality stage of hedonism perfectly explains this behaviour. Contrary to this, there is a strongly held view that hacker cultures are governed by certain universal 'ethical norms' like (a) access to computers should be unlimited and total, (b) all information should be free, and (c) No intentional damage to any system. The internet is replete with hacker manifestos claiming that they subscribe to a higher moral code wherein the authors claim that hacking is actually benefiting mainstream society by exposing the weaknesses of the multinational corporations which is positive social behaviour. Himma (2005) calls this 'hacktivism' or value based hacking. However, it is believed that hacker ethics are never followed and are only put forward as pretensions to present hacking as a socially beneficial activity. Spafford (1990) describes all hacking activity as unethical, immoral and disruptive despite its contribution to security improvements. Wible (2003) believes that while a cohesive hacker community bound by ethical guidelines is no longer dominant, remnants of the old hacker ethic remain and emphasizes on an effort to help rebuild a community of hackers, through rewarding contests, in which a body of positive social norms can be sustained. Still (2006), however, portrays the motivations 'hacktivism' in a positive light

---

<sup>23</sup> See Siegel, *supra* note 7, at p.167.

and states that all hackers are not merely thrill or fame seekers; rather hacktivists are an “organized, technically skilled, politically conscious and socially aware individuals who seek to challenge the authority of oppressive nation states” like China which are engaged in providing state-sponsored information to citizens and curbing the freedom of speech and expression. Thus, the moral development theory provides mixed results.

## **VI. RATIONAL CHOICE THEORY OF HACKING**

The rational choice theory gives primacy to opportunity of crime commission and the willingness of the individual to flout legal norms when he views the outcome as beneficial. However, it is distinct from Akers’s reinforcement theory in portraying crime as a ‘seduction’ i.e. activity capable of producing a natural ‘high’ like drugs in certain individuals. Ferrell (1997) describes it as the “exhilarating, momentary integration of danger, risk and skill” which motivates a person towards criminal behaviour.

### **Hacking as Entertainment: Does Crime Really Seduce?**

Professor Jack Katz (1988), in his revolutionary work *Seductions of Crime*, transgressed the normal social constructs used in formulation of learning and psychological theories to portray crime as the ‘forbidden fruit’. Katz argues that individuals involved in criminal activities actually are engaged in broader efforts to transcend their social environments and though the ‘*transcendence*’ may be transitory yet it produces a strong seduction for evil.<sup>24</sup> A scintillating example is proffered by the account of the well known hacker Kevin Mitnick, presently the CEO of Mitnick Security Consulting.<sup>25</sup> Graobsky (2000) describes the seduction for hacking, from the hacker’s perspective, ‘as an act of power, be gratifying in and of itself’ and beset by the adventure of the ‘exploration of unknown’. Foster (2004) offers anecdotal evidence of computer crime offenders suggesting that the typical computer offender is “almost always male, aged from mid-teens to mid-20s, lacking in social skills, fascinated with technology, an underachiever in other areas (e.g. education)- who sees the computer as a means of being important or powerful”. He also

---

<sup>24</sup> John Hagan, *The Pleasures Of Predation And Disrepute*, 24 Law & Soc’y Rev. 165 (1990).

<sup>25</sup> Mitnick once said “I guess I was curious. I was a very curious kid. I was into like magic. When I was young I was fascinated by magic. I always liked to learn how to do particular illusions and how all these tricks worked.”, retrieved from <<http://www.cartelblanche.co.za/Display/Display.asp?Id=3020>> (Last accessed on July 10, 2007).

proffers evidence that such offenders are generally “unusually bright, eager, highly motivated, courageous, adventuresome and qualified people willing to accept a technical challenge.” Leeson & Coyne (2005) argue that economics of fame-driven hacking is a reality and operates as a “market”; one side of which has the producers of hacks who desire fame. When hackers are better known within the hacker community, they tend to supply a greater quantity of hacking and thus notoriety acts as a prime driving force. An empirically informed study conducted by Orly Turgeman-Goldschmidt(2005) presents the positive attractions of hacking through hackers’ own accounts. She concludes that hackers do not live in a vacuum and equates hacking to a “play”. After an analysis of primary accounts of hacker motivation, she notes:

“For the hackers, then, hacking is a new form of entertainment based on the play-like quality that characterizes the use of digital technology and is a new form of social activity. Hacking can be considered a new form of entertainment that could not have existed before the development of an adequate technology.”

Goldschmidt stresses on the values of individualism viz. individual choice, freedom, and happiness, and argues that being a part of the Western civilization, hackers seek pleasure, fulfilment, and knowledge. The study seems too culture specific and takes a myopic view limited to western civilization only. However, the following salient conclusions from the accounts are noteworthy:

- (I) **Economic Accounts:** Goldschmidt’s accounts, as a rule, focus more on ideology and sideline profit motive which patently is a lopsided conclusion as the desire to make money is associated with specific software piracy offences like trading protected software for profits and such financial motivations are far from hidden.<sup>26</sup>
- (II) **Deterrent Factor:** The probability of being caught and the severity of punishment, if high, may act as effective deterrents. However, she finds that in case of computer related offences both components are low and thus deterrence is negligible.

---

<sup>26</sup> See Peter T. Leeson & Christopher J. Coyne, *supra* note 2.

- (III) **Lack of Malicious or Harmful Intentions:** One of the recurring accounts among the hackers is that they did not have any malicious intent or no harm was actually done. Goldschmidt concludes that many hackers pretend to be morally justified and absolve themselves of harbouring any harmful intentions.
- (IV) **Intangible Offences:** Computer related offences are part of the new breed of offences which are intangible i.e. there is a lack of physical sense of their commission. Thus, the offender cannot feel that the damage has been done, in the physical sense, as the electronic information in computer systems can be stolen without physical interaction. This weighs against the probability of guilt generation.
- (V) **Nosy Curiosity and Voyeurism:** The hackers' accounts point to a voyeuristic curiosity i.e. one driven by seduction of the unknown, the desirable secrets or the confidential. This account is mostly given for offences involving unauthorized browsing through other's files, and justifies Katz hypothesis to a certain extent.
- (VI) **Revenge:** This is a common excuse for offences of virus spreading and crashing computer systems. Revenge is explained, as pointed out below, by Gottfredson and Hirschi (1990) in terms of lower degree of self control in crime-conducive situations.
- (VII) **Ease of Execution:** Hackers, bent on presenting their genius, ability and proficiency, sideline the ease of execution as an explanatory account as it negates their uniqueness. However, the advantage of digital pseudonymity of offender surely reduces the chances of detection.<sup>27</sup>

Thus, a range of multifarious factors is involved in triggering hacker motivations. Lastly, Gottfredson and Hirschi (1990) have linked crime with offender's personality and resultant degree of self control. According to the self-control hypothesis, persons with low self-control are driven away by opportunity of crime commission. Criminal behaviour is therefore mediated on an individual level by the presence of criminal

---

<sup>27</sup> See Neal Kumar Katyal, *Criminal Law In Cyberspace*, 149 U. Pa. L. Rev. 1003 (2001).



opportunity. Individuals low in self-control have a tendency to ignore the long-term consequences of their actions in their decision-making process as well as to be reckless and impulsive, which leads to a greater likelihood of engaging in crime when presented with the opportunity as they cannot resist the seduction of crime. This hypothesis differs from Katz's proposition of commission of crime offering positive rewards like fame and certainly seems applicable in cases of hacking by internal groups.

## **VII. CONCLUSION**

There can never be a perfect 'accounting for all reasons' theory for a new unconventional crime like hacking. As Katsh (1995) puts it, the emerging legal landscape in relation to cyberspace is not very easy to see and thus to understand the changes, it is necessary to "look beyond the surface of law" to recognize "so much that is hidden from view". These latent elements may contribute in structuring the laws and increase their efficacy by providing the missing policy links. A common thread running through all theoretical explanations is the system of 'rewards', both pecuniary and non-pecuniary, to the hackers. It is necessary to efface this system by limiting the ability of big corporations to hire notorious hackers for hefty benefits. Secondly, there is an urgent need to somehow regulate hacker communities operating on the internet. A separate online world has come into existence and governments need to divert their resources to check the growth of hacker cultures through prohibition of hacker magazines and websites. Though such a step may be accused of overreach but ultimately the social benefit will far outweigh the minimal inconvenience caused and in fact, right to speech and expression is subject to the need for social order and classes like 'hacktivists' who claim to represent the voice of subalterns in majoritarian societies cannot claim immunity from general law on moral grounds. Social learning theories emphasize on proper law enforcement as learning essentially takes place through imitation and reinforcements through rewards. Thirdly, there is a need to shed the 'one-size-fits-all' approach in devising punishment schedules as hacker motivations differ over a wide spectrum. Legal responses to crime are ineffective or prove to be worse if they do not account for the social context in which they are applied and are not careful about the social meaning that a particular penalty may convey in that context. A differential targeting of hacker classes, as Leeson & Coyne

(2005) put it, will make the punitive law more effective and rationalized. Lastly, we live in an age of absolute moral uncertainty where no consensus exists about the definitions of right or wrong and the judgmental criteria to place any behaviour in either of the categories. Hacking produces rewards and seduces the youth and the lack of internal controls in form of ethical standards facilitates the commission. Thus, a suggested alternative strategy may include education concerning computer ethics at early stages of school to condition young minds. Active teaching through proper channels induces 'differentiation' capabilities paving way for responsible behaviour. On the whole, there is a need for behavioural sciences to focus more attention on hacking and uncover the distinct motivations for hacking through empirically verified propositions, which traditional criminological theories may not completely explain, and thus contribute towards increasing the efficacy of existing legal regime.

## Selective References

### Articles

- 1) Adamski, A. (1999), "*Crimes Related to the Computer Network, Threats and Opportunities. A criminological perspective*", retrieved from <<http://www.ulapland.fi/home/oiffi/enlist/resources/HeuniWeb.htm>> (Last accessed on July 10, 2007).
- 2) Ferrell, Jeff (1997), "*Criminological Versthen: Inside the Immediacy of Crime*", Justice Quarterly 14(1997), pp.3-23 at 12.
- 3) Fitch, Cynthia (2003), "*Crime and Punishment: The Psychology of Hacking in New Millenium*", retrieved from <[http://www.giac.org/practical/GSEC/Cynthia\\_Fitch\\_GSEC.pdf](http://www.giac.org/practical/GSEC/Cynthia_Fitch_GSEC.pdf)> (Last accessed on July 10, 2007).
- 4) Foster, David Robert (2004), "*Can The General Theory Of Crime Account For Computer Offenders: Testing Low Self-Control As A Predictor Of Computer Crime Offending*", retrieved from <<https://drum.umd.edu/dspace/handle/1903/1536>> (Last accessed on July 10, 2007).
- 5) Grabosky, Peter (2000), "*Computer Crime: A Criminological Overview*", p.19, retrieved from <[http://www.aic.gov.au/conferences/other/grabosky\\_peter/2000-04-vienna.pdf](http://www.aic.gov.au/conferences/other/grabosky_peter/2000-04-vienna.pdf)> (Last accessed on July 10, 2007).
- 6) Himma, Kenneth (2005), "*Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?*", retrieved from <<http://ssrn.com/abstract=799545>> (Last accessed on July 10, 2007).
- 7) Hollinger, R. (1988), "*Computer hackers follow a guttman-like progression*", Social Sciences Review, Vol. 72, pp.199-200.
- 8) Leeson, Peter T. & Coyne, Christopher J., "*The Economics Of Computer Hacking*", 1 J.L. Econ. & Pol'y 511(2005).
- 9) Lemos, Robert (2002), "*New Laws Making Hacking a Black and White Choice*", CNET News, retrieved from <<http://news.com.com/2009-1001-958129.html>> (Last accessed on July 10, 2007).

- 10) Rogers, Marcus (2000), "*Psychological Theories of Crime and Hacking*", retrieved from <<http://homes.cerias.purdue.edu/~mkr/>> (Last accessed on July 10, 2007).
- 11) Rogers, Marcus (2001), "*A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study*", University of Manitoba, Canada.
- 12) Rogers, Marcus (2002), "*A New Hacker Taxonomy*", retrieved from <<http://homes.cerias.purdue.edu/~mkr/hacker.doc>> (Last accessed on July 10, 2007).
- 13) Spafford, Eugene H. (1992), "*Are computer hacker break-ins ethical?*" *Journal of Systems and Software*, 17(1), pp.41–48.
- 14) Still, Brian (2006), "*Hacking for a Cause*", *ICFAI Journal of Cyber Law*, Vol V, No.1, February, 2006, p.22.
- 15) Turgeman-Goldschmidt, Orly (2005), "*Hackers' Accounts: Hacking as a Social Entertainment*", *Social Science Computer Review*, Vol. 23, No. 1, pp.8-23, retrieved from <<http://ssc.sagepub.com/cgi/content/abstract/23/1/8>> (Last accessed on July 10, 2007).
- 16) Wible, Brent (2003), "*A Site Where Hackers Are Welcome: Using Hack-In Contests To Shape Preferences And Deter Computer Crime*", 112 *Yale L.J.* 1577 (2003).

## **Books**

- 1) Gottfredson, M. R. & Hirschi, T. (1990), *A General Theory of Crime*, Stanford: USA.
- 2) Katsh, M. Ethan (1995), *Law in a Digital World*, Oxford University Press: New York.
- 3) Katz, Jack (1988), *Seductions of Crime: Moral and Sensual Attractions in Doing Evil*, New York: Basic Books.