Psychological Theories of Crime and "Hacking"

By Marc Rogers M.A. CISSP, Graduate Studies, Department of Psychology, University of Manitoba

Abstract

This thesis explores the relatively new criminal phenomena of computer crime, or as it is more commonly termed, hacking. The foundation for the examination is based on how well traditional psychological theories of crime and deviance explain this new behaviour. Dominant theories in each of the categories of psychoanalytic, learning and control are discussed. The thesis concludes that for the most part, traditional psychological theories are deficient with regard to explaining criminal computer behaviour. It is argued that differential association and social learning theory may be partially effective in explaining the initial involvement and continuation of criminal computer behaviour.

Psychological Theories of Crime and "Hacking"

Today's society is in the midst of a technological revolution. With advances in computers and telecommunications most businesses and many individuals have become dependent on computers and networks to carry out everyday activities (Howard, 1997; Sterling, 1992). Howard (1997) indicated that as of 1996, 13 million hosts systems were accessing the Internet. It has been estimated that by the year 2003, the number will have risen to well over 200 million (Denning, 1998). The rush to embrace the new technology has also introduced a new category of criminal activity and behaviour, commonly known as hacking[1] (Goodell, 1996; Littman, 1995).

Hacking is a criminal activity that relies on the dependence of computers and networks, including the Internet (Hutchison, 1997, Rasch, 1996; Stoll, 1985). Those individuals engaged in hacking activities have been termed hackers (Howard, 1997; Taylor, 1998). The term hacker has had many connotations over the years. It was originally associated with outstanding and radical programmers in the computer science fields (usually from Berkley, Stanford or MIT) (Chandler, 1996). Today it commonly refers to an individual engaged in a form of criminal behaviour, hacking. Hacking can be formally defined as either a successful or unsuccessful attempt to gain unauthorized use or unauthorized access to a computer system (Howard, 1997).

Society is now attempting to come to grips with this new criminal activity that knows no geographical boundaries and blurs the notion of criminal jurisdiction (Hafner & Markoff 1995; Hutchison, 1997). Behavioural science has been remiss in its research into the phenomena of hacking and as such there has been little or no empirical research in the areas of psychological profiles and causes of the behaviour (Karnow et al., 1994).

---

[1] There have been several debates over the use of the term hacker versus cracker, versus phreaker. Since the term hacking is generic and covers a continuum of behaviors including criminal behaviour, no distinction will be made for the purposes of this paper.

In order to understand the criminal behaviour of hackers, it is necessary to examine the traditional psychological theories of criminal behaviour and how they may be applied to develop an understanding of hacking.

Major Psychological Theories of Crime

The major psychological theories of crime can be categorized into the following areas; psychoanalytic theory learning theory, and control theory (Blackburn, 1993; Feldman, 1993; Hollin, 1989). Dominant theories within each of these categories will be briefly reviewed.

The major psychological theories of crime have been influenced to some extent by other fields (i.e., criminology, sociology, & biology) (Feldman, 1993; Hollin, 1989). Criminology may have had the largest effect on the development of behavioural theories of crime (Bartol, 1991; Hollin, 1989). As such it is important to briefly review the two predominant schools of thought in criminology, classical, and positivist theory. (Clinnar & Quinney, 1986; Feldman, 1993; Hollin, 1989).

The classical theorists hold central the concept that man is capable of free will (Hollin, 1989). Crime can be explained in terms of choices between criminal behaviour (if the opportunity arose) or non-criminal behaviour. If the rewards for a criminal act are greater than the retribution, the probability of criminal behaviour increases (Hollin, 1989).

The positivist theorists believe that the causes of criminal behaviour are outside the realm of free will and are influenced by other factors (Hollin, 1989). The factors range from the biological (genetics), to the sociological (environment) and to the psychological (personality, learning, etc.) (Feldman, 1993). It has been argued that psychological theories are positivist in nature as they all seek to account for criminal behaviour by way of factors outside of the individual's control (Hollin, 1989).

Psychoanalytic Theories

Psychoanalytic theory, as developed by Freud, has taken a somewhat indirect approach in explaining criminal behaviour. It relies on the pathological process by which criminal acts are thought to be manifested (Blackburn, 1993).

Freud believed that there was an inner moral agency (superego) governing conduct, whose development depends primarily on satisfying parent-child relationships (Blackburn, 1993). Inadequate superego formation and function accounts for criminal behaviour (Blackburn, 1993). Behaviour therefore depends on the balance of the psychic energy system. A disturbance in this system or any component structure produces maladaptive development (Blackburn, 1993).

The work of August Aichhorn is one of the first formal psychoanalytic attempts at understanding criminal behaviour (Hollin, 1989). Aichhorn stated that there was some underlying predisposition termed "latent delinquency", that resulted in a child becoming a criminal later in life (Hollin, 1989). He believed that each child was typically asocial in its first dealings with the world and due to a failure in psychological development this asocial tendency (latent delinquency) persisted and governed behaviour resulting in the criminal behaviour (Hollin, 1989).

Other 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 (Feldman, 1993; Hollin, 1989).

Sublimation has also been offered as a factor for an individual engaging in criminal behaviour (Blackburn, 1993; Hollin, 1989). The criminal act is thought to result from inner unsatisfied wishes, which in turn stem from a failure to express strong emotional ties with another person, often the parent (Hollin, 1989).

Although there are other psychoanalytic theories of crime (maternal deprivation, low self-esteem), the length restriction on this paper prevents a more in depth review.

Psychoanalytic theories of crime stress the role the inner processes and conflicts play on the determinants of behaviour (Blackburn, 1993; Hollin, 1989). Blackburn (1993), summed up the psychoanalytic theory of crime as subscribing to three claims: (1) socialization depends on the internalization of society's rules during early childhood; (2) impaired parent-infant relationships are causally related to later criminal behaviour; (3) unconscious conflicts arising from disturbed family relationships at different stages of development are the causes of some criminal acts.

Psychoanalytic theories of crime are primarily suited for those types of crimes that result from unconscious conflicts (Blackburn, 1993; Hollin, 1989). They are not well suited for explaining crimes that incorporate planning and rational goals such as, white collar and computer crimes[2] (Blackburn 1993; Feldman, 1993; West, 1988).

Learning Theories

Differential Association

Learning theory approaches to explaining criminal behaviour have links to one of the core sociological theories of crime, the differential association theory (Blackburn, 1993; Gattiker & Kelly, 1977; Hollin, 1989). Differential association as described by Sutherland (1947) is based on the notion that modern society contains conflicting structures of norms and behaviours. It also contains conflicting definitions of appropriate behaviour that give rise to crime (Blackburn, 1993; Feldman, 1993; Gattiker & Kelly, 1997; Hollin, 1989). Normative conflict at the individual level is translated into individual acts of delinquency through differential association learned through communication usually in intimate groups (Sutherland, 1947). In other words peer pressure and peer attitudes influence behaviour (Blackburn, 1993; Hollin, 1989).

Contact with persons who have favourable definitions toward crime, leads to an individual learning similar definitions (Hollin, 1989). The theory does not indicate that the persons being associated with have to be criminals, they only have to express favourable attitudes toward crime (Hollin, 1989).

Operant Conditioning

B.F. Skinner's theory of operant conditioning holds as one of its principles, that behaviour is determined by the environmental consequences it produces for the individual involved (Blackburn, 1993; Hollin, 1989). Behaviour that produces consequences that are desirable will increase in frequency. The behaviour is said to be reinforced (Blackburn, 1993; Hollin, 1989). Behaviour, which produces undesirable consequences, will decrease in frequency. The behaviour is being punished (Hollin, 1989). Behaviour therefore operates on the environment to produce results that are either reinforcing or punishing.

If the consequences of a person engaging in criminal activity were rewarding (i.e., increase in prestige, money, or feelings of adequacy) the person is likely to engage in further criminal activity (Feldman, 1993). If the consequences were negative (i.e., being arrested, shunned, etc.) the frequency of future criminal behaviour should be reduced (Blackburn, 1993).

Operant conditioning has been used to explain general delinquency as opposed to focusing on specific offences (Blackburn, 1993).

Differential Reinforcement

The theory of differential reinforcement stems from Sutherland's idea that learning was a component of criminal behaviour, and Skinner's theory of operant conditioning (Blackburn,

---

[2] The psychoanalytic theories are falling out of vogue and are being replaced by learning and control theories (Agnew, 1995; West, 1988).

1993; Hollin, 1989). The theory agrees that criminal behaviour is learned through the various groups and associations an individual maintains (Blackburn, 1993). The behaviour then continues or is maintained directly by the consequences of the act as in operant conditioning (Blackburn, 1993).

The theory states that a criminal act occurs in an environment in which the individual has, in the past, been reinforced for behaving in such a manner, and the negative consequences of the behaviour have been minor enough that they do not prevent the response (Hollin, 1989). Due to the fact that criminal behaviour can result in differing schedules of reinforcement and punishment (e.g., being caught, etc.), the behaviour is subject to a somewhat complex learning history (Blackburn, 1993). The result being that the criminal behaviour is hard to extinguish (Feldman, 1993).

The use of differential reinforcement theory in understanding criminal behaviour has historically centred on stealing and property related offences (Blackburn, 1993; Feldman, 1993; Hollin, 1989). These offences fit nicely into the theory as the gains from such activity unless the individual was arrested, are positive (e.g., more money, avoiding poverty, etc.).

Social Learning Theory

Social learning theory in psychology, is generally associated with the work of Albert Bandura and his research on modelling, and imitation (Ewen, 1980; Feldman, 1993; West, 1988). Social learning theory postulates that behaviour can be learned at the cognitive level through observing other people's actions (Blackburn, 1993; Feldman, 1993; Hollin, 1989). People are capable of imagining themselves in similar situations, and of incurring similar outcomes (Ewen, 1980). Once the behaviour is learned it may be reinforced or punished by the consequences it generates. Bandura subscribed to several of the essential concepts of the operant conditioning theory; reinforcement, punishment, and motivation (Feldman, 1993).

Bandura believed that there were three aspects to motivation. He termed these external reinforcement, vicarious reinforcement, and self-reinforcement (Ewen, 1980; Feldman, 1993; Hollin, 1989). External reinforcement was similar to Skinner's concept of reinforcement. Vicarious reinforcement was derived from observing other people's behaviour being either reinforced or punished. Self-reinforcement refers to ones' sense of pride, or as meeting of standards in ones' own behaviour (Ewen, 1980).

According to social learning theory, criminal behaviour is acquired through observational learning. The learning takes place in three contexts, the family, prevalent subculture, and the social environment (Ewen, 1980; Feldman, 1993; Hollin, 1989). The reinforcement for criminal behaviour comes from both the internal and external sources. The reinforcement can be in the form of tangible rewards of the criminal activity itself (i.e., money), or from social rewards (i.e., increase in peer status) (Blackburn, 1993; Hollin, 1989).

Criminal behaviour is maintained through a complex schedule of reinforcement and punishment throughout the life of the individual (Feldman, 1993). This is similar to the differential reinforcement concept of factors influencing criminal behaviour. According to the theory, if criminal behaviour has been reinforced in the past, there is an expectancy that it will be reinforced in the future (Hollin, 1989).

Social learning theory has primarily been used to understand aggressive behaviour and aggressive or violent criminal offences such as assaults or robbery (Hollin, 1989).

Control Theories

Theories falling under the umbrella of control theory share a common underlying assumption. The assumption is that everyone has the potential to engage in criminal behaviour (Blackburn, 1993). Control theory does not focus on why do a few people commit crimes, but on why doesn't everyone commit crimes (Agnew, 1995; Hollin, 1989; West, 1980).

Moral Development (Kohlberg)

Kohlberg believed that socialization is a process that is linked to moral development. Kohlberg's theory of moral development postulates that moral reasoning develops in a sequential manner as the person matures. The theory breaks the development into three

levels containing two stages at each of the levels (Hollin, 1989). Moral reasoning develops from the concrete at the lower stages to the more abstract at the higher levels. The abstract includes such concepts as justice, rights, and principles (Blackburn, 1993; Hollin, 1989).

Criminal behaviour arises when an opportunity to offend occurs and there is a delay in the development of moral reasoning in the individual (Hollin, 1989). The individual cannot control the temptation to engage in the activity and offends. The theory is more suited for understanding general delinquency and possibly white-collar and corporate crime (Balckburn, 1993; Clinnard & Quinney, 1986).

Eysenck's Theory

Eysenck's theory of crime stems from his work on personality (Blackburn, 1993; Eysenck, 1977; Hollin, 1989). The theory is based on the notion that through heredity some individuals are born with cortical and autonomic nervous systems which effect their ability to be conditioned by environmental stimuli (Blackburn, 1993; Eysenck, 1977; Hollin, 1989). The theory recognizes that an individual's behaviour is influenced by both biological and social factors (Blackburn, 1989; Eyesenck, 1977).

The theory initially defined two dimensions of personality, extraversion (E), and neuroticism (N). These dimensions existed on a continuum with most people falling in the middle range of possible scores (Eysenck, 1977; Hollin, 1989). The extraversion dimension ranged from high (extravert) to low (intravert). The neuroticism dimension ranged from high (neurotic), to low (stable). Eysenck later added a third dimension, psychoticism (P) (Eysenck, 1977). The P dimension or scale was thought to measure attributes such as aggression, preference for solitude, and lack of feelings for others (Hollin, 1989).

According to Eysenck's theory, children learn to control antisocial behaviour through the development of a conscience. The conscience is a set of conditioned emotional responses to environmental stimuli associated with antisocial behaviour (Eysenck, 1977; Hollin, 1989). An example of the conditioning would be receiving punishment from a parent for some antisocial act. The conditioning socializes the child (Blackburn, 1993; Eysenck, 1977; Hollin, 1989).

Both the speed and the efficiency at which the conditioning process occurs, (conditionability), is dependent on the individual's temperament expressed in terms of extraversion (E), and neuroticism (N) (Blackburn, 1993; Eysenck, 1977). High E high N combinations led to poor conditionabilty, and therefore poor socialization and an inclination towards criminal behaviour (Blackburn, 1993; Eysenck, 1977). Low E low N on the other hand would lead to good conditionability and effective socialization (Eysenck, 1977; Hollin, 1989). High scores on the third dimension psychoticism (P) would indicate a hostility towards others and an inclination to more aggressive, violent criminal behaviour (Eysenck, 1977).

Eysenck's theory is geared more toward anti-social behaviour, and has had mixed results in predicting general deviancy (Hollin, 1989).

Theories and Hacking

There does not appear to be any one theory that accounts for all types of the more conventional criminal behaviour (Blackman, 1993; Ellison & Buckhout, 1981; Hollin, 1989). This problem is compounded when dealing with unconventional criminal activity such as hacking (Hutchison, 1997; Post, 1996). The term hacker doesn't refer to a single homogeneous group (Post, 1996; Power, 1996). The limited empirical research into this behaviour indicates that there are various sub-groups under the hacker umbrella (Howard, 1997; Post, 1996). These subgroups can be ordered from novices up to professional criminals (Post, 1996; Power, 1996). The subgroup the hacker would be classified as depends on the motives and causes behind the behaviour (Post, 1996).

At best some of the traditional theories reviewed can only be applied to a limited portion of the theorized hacker subgroups. The psychoanalytic theories concentrate mainly on unconscious factors and the child-parent interactions (Blackburn, 1997). Although several of the more infamous hackers have come from dysfunctional families, this is not sufficient to

explain their choice of the criminal activity to engage in (Goodell, 1996; Hafner & Markoff, 1995; Littman, 1995; Littman, 1997).

Psychoanalytic theories are not adequate at explaining criminal behaviour that is planned out (Blackburn, 1993). Hacking is such an activity, as it requires a specific skill set, familiarity with computers, networks and a relatively advanced technological understanding (Garfinkel & Spafford, 1996; Howard, 1997). To be successful at hacking the individual also has to plan the attack in some detail (Garfinkel & Spafford, 1996; Goldstein, 1997). The attacks are deliberate and the victim system or networks are usually pre-chosen and not random (Howard, 1997; Littman, 1995).

The success of control theory in explaining hacking is mixed. Eysenck's theory on personality and crime would predict that hackers should be high on the extraversion scale. The majority of the arrested hackers and those, which have responded to surveys, indicate they are withdrawn, uncomfortable with other people and are intraverts (Littman, 1997; Post, 1996).

Moral development theory may be more useful in understanding a subset of hackers. According to Kohlberg's theory on moral development, one of the pre-morality stages is hedonism (Hollin, 1989). There have been many documented anecdotal accounts of the lack of concern by hackers over the systems they have attacked (Goodell, 1996; Littman, 1995). Many of the written interviews with convicted hackers portray them as being more concerned with fulfilling their own material needs regardless of the consequences (Littman, 1997). However, there has been no empirical evidence available to support this assumption.

There is some evidence to suggest that certain hackers may subscribe to a moral code that is very abstract and would definitely be considered to be at Kohlberg's 6th and last stage of development, universal ethical principles (Blackburn, 1993). The Internet is replete with hacker manifestos claiming they subscribe to a higher moral code. The authors claim that hacking is actually benefiting mainstream society and that exposing the weaknesses of the multinational corporations is positive social behaviour (Duff & Gardner, 1996; Goldstein, 1997; Mizrach, 1997; Sterling, 1992).

The learning theories may have the best chance at providing an understanding of hacking (Rogers, 2001). However, Skinner's operant conditioning theory by itself cannot account for this behaviour. Hackers who have been caught and repeatedly punished, with no obvious reinforcement, still continue to engage in the activity as though it were a compulsion (Gattiker & Kelly, 1997; Hafner & Markoff, 1995; Post, 1996).

Social learning theory and differential reinforcement seem to be more appropriate to extend to hacking behaviour than the other traditional theories. 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.
Although hackers are self-reported loners and have underdeveloped traditional social skills, they appears to be a strong desire for affiliation and need for peers [3](Littman, 1997; Post, 1996; Sterling, 1992). Hackers tend to associate with other individuals who also engage in hacking behaviour. These associations can take the form of purely electronic, as in online chat sessions, or more intimately by joining a hacking club (e.g., Cult of the Dead Cow CDC, Legion of Doom) (Goodell, 1996; Littman, 1997; Sterling, 1992). The hackers even hold conventions such as the recent Defcon in Las Vegas, where they share ideas, techniques, and intelligence information.

It is also evident that the hackers are learning their respective criminal behaviour, and are doing so amongst individuals who hold positive attitudes toward such behaviour (Sterling, 1992).

The continuation of hacking may be due to several reinforcing factors. The reinforcement derived from hacking may come from the increase in knowledge, prestige within the hacking community, or the successful completion of the puzzle (some hackers indicate that to them attacking a system is a type of game) (Hafner & Markoff, 1995; Taylor, 1998). In

---

[3] Current studies indicate that hackers may have well developed social skills, but these skills are non-traditional and are centered around computer mediated interactions (i.e., chat groups, news groups etc.)

some rare cases prestigious companies have hired hackers who have penetrated their systems (Goodell, 1996; Hafner & Markoff, 1995; Littman, 1995). This has led to the large-scale myth that hackers can "land" good jobs in the computer security industry (Littman, 1997). Such a myth can definitely be seen as reinforcing.

Other reinforcing aspects of hacking include the fact that the media is enamoured with the romantic notion of hackers, and is turning some into celebrities (Littman, 1995; Power, 1996). An Israeli youth charged with attacking US Military networks was given a lucrative promotional contract with a European computer manufacturer, and was praised by the Prime Minister of Israel for his ingenuity (Wired, 1998).

The negative aspects of hacking, such as being arrested, has been seriously undermined by the lack of stiff sentences. In Canada, the average sentence for the offence of unauthorized use of a computer service is alternative measures for a youth, and a conditional discharge for an adult (Rogers, 2001).

According to the differential reinforcement theory then, the hacking behaviour should continue as it is being reinforced (Hollin, 1989). Howard (1997) provides support for this in his research into hacking incidents in the US during the period of 1989-95. He concluded that the number of hacking incidents is not decreasing, but increasing at a rate proportional to the increase in systems connecting to the Internet.

Bandura's social learning theory can also be used to understand the behaviour of hacking (Rogers, 2001). The theory states that criminal behaviour is acquired through observational learning, and the reinforcement from the behaviour comes from external and internal sources (Blackburn, 1993). As previously stated, hacking is behaviour in which imitation and modelling seem to play an important role (Chandler, 1996; Goodell, 1996). The hacking underground has also been likened to a subculture, which reinforces adherence to its own moral code (Hafner & Markoff, 1995; Mizrach, 1977; Taylor, 1998). Part of the code is sharing information on attacks and the mentorship of "newbies" (i.e., individual just starting to learn how to attack systems) (Taylor, 1998).

Maintenance of the hacking behaviour may be due to complex reinforcement schedules, which would be in keeping with the social learning theory's model as well.

Conclusions

The lack of theories dealing specifically with hacking behaviours, may in part be due to the relative newness of this behaviour. Hacking is a criminal activity that is somewhat unique and dependent on the rather recent development of computer and network technology, including the Internet (Howard, 1997; Taylor, 1998).

The major traditional psychological theories crime fall woefully short of explaining all of the hacking behaviours (Rogers, 2001). Certain theories such as Kohlberg's moral development theory, differential reinforcement theory, and social learning theory, appear to be useful in explaining how the initial behaviour may be acquired and then maintained (Rogers, 2001). Unfortunately behavioural science has yet to focus much attention on hacking despite the fact that hackers have received a large amount of attention by the media and the government (Power, 1996).

Before any meaningful empirical research can be done, a better taxonomy of this complicated behavopur needs to be developed. The current method of categorizing all persons involved in various computer specific criminal activities into the one generic category of "hackers", holds little utility (Post, 1996; Rogers, 2001). Meaningful subgroups need to be developed and operationally defined, before a better understanding of this criminal behaviour can be accomplished.

References

Agnew, R. (1995). Testing the leading crime theories: An alternative strategy focusing on motivational processes. Journal of Research in Crime and Delinquency, 32, 363-398.

Bartol, C. (1991). Criminal behavior a psychosocial approach 3rd edition. New Jersey: Prentice Hall.

Blackburn, R. (1993). The psychology of criminal conduct: Theory, research and practice. Toronto: John Wiley & Sons.

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

Clinard, M. & Quinney, R. (1986). Criminal behavior systems: A typology 2nd edition. Chicago: Pilgrimage.

Denning, D. (1998). Information Warfare and Security. Reading: Addison-Wesley.

Duff, L., & Gardiner, S. (1996). Computer crime in the global village: Strategies for control and regulation- in defence of the hacker. International Journal of the Sociology of Law, 24, 221-228.

Ellison, K. & Buckhout, R. (1981). Psychology and criminal justice. New York: Harper & Row.

Eysenck, S. & Eysenck, H. (1977). Personality differences between prisoners and controls. Psychological Reports, 40, 1023-1028.

Ewen, R. (1980). An introduction to theories of personality. New York: Academic Press.

Feldman, P. (1993). The psychology of crime a social science textbook. Cambridge: Cambridge University Press.

Garfinkel, S., & Spafford, G. (1996). Practical unix and internet security. New York: O'reilly & Associates Inc.

Gattiker, U., & Kelley, H. (1997). Techno-crime and terror against tomorrow's organization: What about cyberpunks? Available HTTP: www.ncsa.com/library.

Goldstein, E. (1997). And justice for all. 2600: The Hacker Quarterly, 13(2), 48-57.

Goodell, J.,(1996). The cyber thief and the samurai. New York: Dell Publishing.

Hafner, K. & Markoff, J. (1995). Cyberpunks: Outlaws and hackers on the computer frontier. Toronto: Simon and Schuster.

Hollin, C. (1989). Psychology and crime: An introduction to criminological psychology. New York: Routledge

Howard, J. (1997). Analysis of security incidents on the internet. Unpublished doctoral dissertation, Carnegie Mellon University, Pennsylvania.

Hutchison, S. (1997). Computer crime in canada. Unpublished Manuscript.

Karnow, C., Landels, R. & Landels, D. (1994). Recombinant culture: crime in the digital network. Available HTTP: www.cpsr.org/privacy.

Littman, J. (1995). The fugitive game: online with kevin mitnick. Toronto: Little Brown & Company.

Littman, J. (1997). The Watchman: The twisted life and
crimes of serial hacker kevin poulsen. Toronto: Little Brown & Company.

Mizrach, S. (1997). Is there a hacker ethic for the 90s? Available HTTP: Hostname: infowar.com.

Post, J. (1996). The dangerous information system insider: Psychological perspectives. Available HTTP: www.infowar.com

Power, R. (1996). Testimony before the permanent
subcommittee on investigations. Available HTTP: www.gocsi.com/preleas2.

Power, R. (1998). Current and future danger. Computer Security Institute.

Rasch, M. (1996). Criminal law and the internet. The
Internet and Business: A Lawyer's Guide to the Emerging Legal issues. Available HTTP: www.cla.org/RuhBook/chp11.htm

Rogers, M. (2001). A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study. Unpublished dissertation.

Stoll, C. (1985). The cuckoos egg: Tracking a spy through the maze of computer espionage. New York: Mass Market Paperback.

Sutherland, E. (1947). Principles of criminology (4th ed.). Philadelphia: Lippincott.

Taylor, P. (1998). Hackers: the hawks and the doves-enemies & friends. Unpublished manuscript.

West, D. (1988). Psychological contributions to criminology. British Journal of Criminology, 28, 77-92.

Wired News. (1998). Analyzer takes notoriety to the bank. Available