A CONCEPTUAL MODEL OF HACKER DEVELOPMENT AND MOTIVATIONS

John Van Beveren
University of Ballarat, Australia

ABSTRACT

A conceptual model describing the development of hackers and their motivations is constructed from existing psychological theories. The constructs of "flow" and "criminal tendency" are taken and developed from psychological theories of motivation and learning. These constructs are used as moderators and mediators respectively in the model to describe the development of a hacker from "Tool kit/Newbie" to "Cyber Punk" or "Old Guard" as described in Rogers (2001) taxonomy of hackers. Empirical testing of the model has not been achieved in this paper. However if empirical testing does support the model then the constructs involved may provide website designers, network administrators and managers with useful variables and insights to reduce hacker development.

INTRODUCTION

The Internet and Web technologies have provided ease of access to information and an efficient communication channel for those who use it. However the ease of use and access to information has fostered new category of criminal activity and behaviour, which is commonly referred to as hacking.

The term hacking or hacker has been used broadly to incorporate the intention by individuals or groups to cause havoc over the Internet; either by infiltrating sites, releasing viruses or causing denial of service

On computers rendering them inoperable. The intentions of hackers and the acts themselves have been the result of various motives and caused various outcomes.

Many researchers and journalists have provided descriptive accounts of hacker's motivations and developed profiles from interviews and surveys of those that have been apprehended. However behavioural scientists have provided little or no empirical research in the areas of psychological profiles and causes of hacking behaviour (Karnow et.al, 1994). A notable exception is Rogers (1999) who provided a review of the limited research that had previously been conducted and introduced new hacker taxonomy.

The theories he reviewed were mainly from major psychology and sociology theories of crime, and were used to understand the criminal behaviour of hackers. Rogers concluded that for the most part traditional psychological theories are deficient with regard to explaining criminal computer behaviour. This could be due in part to the perceptions of the virtual environment by the public and hackers as compared to criminal activity in the physical world. Therefore a theory, which has its foundations in traditional psychological theories and incorporates the enduring attraction of the virtual environment to hackers, is needed.

The Web has created a virtual world, and as such is viewed by many as being separate to physical world in which we live. This view on the one hand separates it from most people's psyche, but to others it has created an alternative, an alluring prospect, particularly when the physical world does not provide the needs, wants and a sense of participation as it does for most.

The alluring nature of the Web and computer mediated environments has been studied by many in the fields of consumer behaviour, marketing, computer science, and psychology. In particular there has been a quest for discovering what makes computer- mediated environments compelling places that attract people's interest. Some of this research has focused on the question of what motives people to engage in the human-computer interaction to the state where their involvement in the activity focuses their attention to the point where that the physical environment and time become obscured in their conscious state. Some theorists refer to this state as the "flow" (Csikszentmihalyi, 1990).

The purpose of this paper is to develop a model of hacker development from the traditional theories of psychology as reviewed by Rogers, and a theory motivation in human-computer interactions, in particular the flow construct.

LITERATURE REVIEW

TAXONOMY OF HACHERS

Many have suggested that hackers are not a homogenous group (Taylor, 1999; Denning, 1998; Post, 1996; Sperling, 1992). Post (1996) suggested that the term hacker is too broad to be useful for empirical research and that it describes the activity but does not accurately reflect the differences in those who are involved in the activity of hacking.

Rogers (1999) used the findings related to hacker's motivations from work conducted in the security industry and available research to categorized hackers into seven groups. The categories are distinct (although not mutually exclusive) groups that include: "Tool kit/Newbies (NT), cyberpunks (CP), internals (IT), coders (CD), old guard hackers (OG), professional criminals (PC) and cyber-terrorists (CT). These categories are seen as a continuum from lowest technical ability (NT), to highest (OG-CT)" (Rogers, 1999, p.5)

Tool kit/Newbies are those people who are at the initial stages of hacking. They have limited amounts of skill in programming or computing and often gather their information from websites where more developed hackers have published their exploits along with the tools they have developed to conduct their attacks.

Cyber punks are intentionally engaged in malicious acts of defacing web pages and sending junk mail or viruses. They have a little more programming skills than Newbies and thus can write their own programs to attack sites.

The disgruntled employee or ex-employee who is quite computer literate and has some technical knowledge and who hacks into or attacks their employers computer systems is classified in the internal group. He/she may use the privileges or knowledge they were given as part of their role in the firm to attack the firm's computer network. Of all computer related criminal activity, 70% is conducted by this group (Power, 1997).

The old guard hackers are those that have high levels of skill and understanding of computer systems and programming, and are not malicious in their intent. They are mostly interested in the intellectual endeavour. However, Taylor (1999) and Parker (1998) have noted an alarming disrespect for personal property from this group.

The professional criminal and the computer terrorist are the most dangerous group. They are highly skilled, have the latest technology and often hire themselves out as mercenaries for corporate or political espionage.

PSYCHOLOGICAL THEORIES

The major psychological theories of crime can be categorized into the areas of: psychoanalytic theory (Blackburn, 1993), learning theory (Feldman, 1993) and control theory (Hollin, 1989). To some extent, these theories been influenced by other fields such as sociology and criminology (Feldman, 1993; Hollin, 1989).

However, as noted by Rogers (1999) after reviewing those theories, "there does not seem to be any one theory that accounts for conventional criminal behaviour (Blackman, 1993; Ellison & Buckhout, 1981). The issue then becomes even more compounded when dealing with unconventional criminal activity such as hacking (Hutchison, 1997; Post, 1996)" (Rogers, 1999).

Whilst the psychological theories do not seem to account for the behaviour of hackers, there are some important generalizations that can be made from the theories that could help to explain why people might develop criminal tendencies in online environments as they develop their skills. Firstly the lack of negative consequences for those who have been caught hacking has been noted, with many criminals receiving minimal or no sentence. Secondly hacker behaviour is being reinforced through both the computer criminals creating their own communities to encourage each other and the media at times glorifying such behaviour. This adds to the view that our modern society is creating more conflicting structures of norms and behaviours.

The theories also indicate that there is probably some underlying tendency that disposition a person to commit crime, in this paper we refer to this factor as "criminal tendency". The actual cause of criminal tendency is difficult to determine, as has been discussed in the psychological theories. However if we agree that there is such an underlying tendency, then we might be able to assume that the tendency draws an individual hacker toward criminal and malicious activity in their development of hacking skill.

MOTIVATION

Jordan and Taylor (1992) identified a number of motivational themes to hacking behaviour through interviews with individuals in the hacking community, such as: compulsion to hack, curiosity, control and attraction to power, peer recognition and belonging to a group.

Hackers often claim to be addicted to computers and/or to computer networks, where they are compelled to hack. They are curios as to what can be found on the worldwide network and this becomes a frequent topic of discussion in their communities; the more secure or exotic the target of the hack is, the more an unending search for more secure and more exotic targets is reinforced.

Hackers often claim that the thrill of illicit searches in online environments is more exciting than their offline life. Hackers often comment on their powerless offline life often in contrast to the control they may have online over the computer systems of major military or corporate institutions. Community peer recognition from other hackers is gained through involvement in the activity of hacking, and often they discuss their exploits to future computer users or to owners of computer networks that they have identified security loopholes in.

The first three motivational themes to hacking as mentioned above are similar to the antecedents for the construct of flow as described by Webster, et.al. (1993). Therefore we would suggest that the achievement of flow is possibly a moderator for the further development of a hacker from a Tool kit/Newbie to a higher-level hacker. Therefore we need to understand the determinants of flow to gain an understanding of how we might stifle such development and contain the activity of hacking.

FLOW

Flow is a metaphor used by many to describe the sense of effortless action felt when being highly involved in an activity to the degree that attention becomes ordered, fully invested and time is obscured by the involvement in the activity (Csikszentmihalyi, 1997). Flow tends to occur when one faces a clear set of goals that require appropriate responses, and immediate feedback is provided, which leads the person to continue to be involved with the activity.

The construct of flow was pioneered by Csikszentmihalyi (1977) and has been studied in a broad range of contexts including sports, work, shopping, games, hobbies and computer use (Csikszentmihalyi 1977, 1990, 1997; Csikszentmihalyi and Csikszentmihalyi 1988; Csikszentmihalyi and LeFevre 1989). During these activities an individual's skills are fully involved in overcoming the challenges presented from the activity. Csikszentmihalyi (1977) defined flow in terms of the congruence of skills and challenges. Csikszentmihalyi (1990) noted that flow is a useful construct for describing more general human-computer interactions.

According to flow theory, flow can occur when an activity challenges the individual enough to encourage playful, exploratory behaviours, without the activity being beyond the individual's reach. Csikzentmihalyi (1977) proposed that if the activity is too demanding then it may produce anxiety or if it is not challenging enough boredom might be the result rather than flow.

Flow theory suggests that flow is characterized by four dimensions (Csikzentmihalyi 1977; Csikzentmihalyi & LeFevre 1989; Malone 1980). According to Trevino and Webster (1992), within the human-computer interaction experience, flow incorporates the extent to which (a) the user perceives a sense of control over the computer interaction, (b) the user perceives that his or her attention is focused on the interaction, (c) the user's curiosity is aroused during the interaction, and (d) the user finds the interaction intrinsically interesting.

CONTROL

Control is a very important element of flow (Csikszentmihalyi, 1977). Individuals must experience feelings of control over computer interactions for the activity to encourage playful, exploratory behaviour. The interactivity of the Web provides feedback to the individual in a way that is

not possible with more static technologies. The Web provides the individual with control by providing explicit choices among alternatives (Malone & Lepper, 1987).

ATTENTION FOCUS

Attention is focused on an involving activity. In flow the individual's focus of attention is narrowed to a limited stimulus field, filtering out irrelevant thoughts and perceptions; the individual loses self-consciousness, becomes absorbed in the activity and becomes more intensely aware of his or her own mental processes (Csikszentmihalyi, 1977). Webster (1989) found that computer users have reported being "mesmerized" during computer interactions.

CURIOSITY

Malone (1981) suggested that during flow, an individual's sensory or cognitive curiosity is aroused. Sensory curiosity may be aroused through varied, novel and surprising stimuli (Berlyne 1960). The Web environment can encourage sensory curiosity through aesthetic qualities of websites or through hyper-links that provide options that encourage exploration (Rayport and Jaworski 2000).

INTRINSIC INTEREST

Individuals in flow find the activity intrinsically interesting (Csikszentmihalyi, 1977). That is, they are involved in the activity for its own pleasure and enjoyment rather than for some utilitarian purpose.

THE MODEL AND PROPOSITIONS

From the literature many constructs have been identified that relate to the development of hackers, and the motivational aspects for such development. It has been suggested that one construct, that of flow, might be a moderator in the development of a hacker from a "Newbie" to a higher-level hacker. Therefore we have developed a model that incorporates the development of a hacker as shown in figure 1.

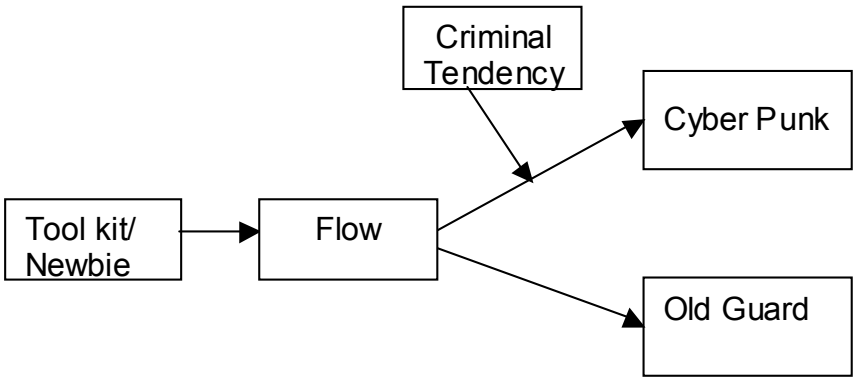

Figure 1: A Model of Hacker Development

The assumptions of this model are that most people who become hackers begin as Tool kit/ Newbies and then develop into cyberpunks or old guard type hackers. This is based on the fact that more skill and experience is required to reach the level of cyberpunk or old guard. It is also assumed that Internals have specific knowledge of the organization and as such may only be inclined to hack when they become disgruntled and therefore do not go through the development stages of other hackers. The other levels of hacker: professional criminals and computer terrorists may develop from cyber punks but for simplicity we will concentrate on the development of new hackers from Tool kit/ Newbies to either Old Guards or Cyber Punks.

From the model it is assumed that Tool kit/ Newbies gather information from published materials such as books, magazines or other hacker's or hacker group's websites and that from such information they develop their knowledge. An integral part of this process is that the Tool kit/Newbie must try to develop their skill and receive positive feedback by using the tools and information they have gathered. Therefore the first proposition is that:

PROPOSITION 1

The tool kits and information gathered by the Newbie must be successful to provide positive feedback to the hacker

The gathering of such tools and information with successful results then leads the hacker to repeat the behaviour therefore engaging the individual in more of the same activity. The Newbie will then develop his or her confidence and so seek more challenge in the activity and therefore seek new tools to meet the new challenge. If the pattern of receiving positive feedback in each attempt then the hacker will begin to achieve the state of flow. This is because each challenge requires new skills and as the hacker is able to develop such skills, he/she will seek new challenges. Therefore the achievement of flow will lead to further hacking.

The achievement of flow may ultimately lead the Newbie to develop enough skill to be reclassified as a Cyberpunk or Old guard depending on the result of the activity by the hacker and his/her goals from the activity.

PROPOSITION 2

The development of skills to meet new challenges is dependent on the available tools and challenges within the online environment.

PROPOSITION 3

Where sufficient challenges and matching tools to develop skills are present flow will occur within the individual.

PROPOSITION 4

A Newbie becomes a Cyberpunk or Old guard through the development of sufficient skills.

PROPOSITION 5

Experiencing flow rapidly increases the motivation to develop skills and find more challenges.

As discussed earlier criminal tendencies might be present within an individual, and these tendencies would draw the individual to engage in activities to produce malicious or criminal outcomes.

PROPOSITION 6

Criminal tendencies present in the individual would draw a Newbie hacker toward Cyber punk activities rather than Old guard activities as hacking skills are developed.

CONCLUSIONS

This model provides a theoretical framework for further empirical analysis of the stages of hacker development. If the model is supported with empirical findings, then the flow construct would offer some important variables which website designers, network administrators and managers could consider when developing network security policies and designs.

The flow construct has several important determinants. Firstly, the congruence between challenge and skill provides an important insight into the interaction of a hacker's ability and the information provided from hacker websites. Similarly the curiosity, focused attention and control factors attributed to the flow state offer insights to the conditions that fulfil many of the reported needs of a hacker.

Network administrators, designers and managers might use these insights to develop policies that reflect the need to patch holes reported by software venders and hackers so that hacking by Newbies is stifled. This would require a consistent and collective effort of those who manage networks. Similarly network tools and techniques available to hackers are also available to network administrators. Therefore network administrators need to be aware of and up to date with the development of such tools for Newbie hackers.

The more holes that are patched, bugs that are fixed and networks that are tightened up the less available the environment will be for hackers to develop their skills. Therefore if the challenge is beyond the Newbie hacker then the less likely he/she is to achieve flow and therefore the less likely to develop their skill. Understanding hackers is one thing, actually doing something proactive requires a joint effort of those responsible for the networks that hackers attack.

REFERENCES

Bandura, A. (1977). "Self-efficacy: Toward a unifying theory of behavioural change", *Psychological Review,* Vol.**84,** 191-215.

Berlyne, D.E. (1960). *Conflict, arousal, and curiosity* New York: Mc Graw-Hill.

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

Csikszentmihalyi, M. (1977). *Beyond Boredom and Anxiety*, San Francisco: Jossey-Bass.

Csikszentmihalyi, M. (1990). *Flow: The Psychology of Optimal Experience*, New York: Harper & Row.

Csikszentmihalyi, M. (1997). *Finding Flow: The Psychology of Engagement with Everyday Life*, New York: Basic Books.

Csikszentmihalyi, M. and Csikszentmihalyi, I. S. (1988). Introduction to part IV. In *Optimal Experience: Psychological Studies of Flow in Consciousness.* Mihlay Csikszentmihalyi and Isabella Csikszentmihalyi ed. Cambridge, UK: Cambridge University Press.

Csikszentmihalyi, M. and LeFevre, J. (1989). "Optimal Experience in Work and Leisure", *Journal of c Personality and Social Psychology,* Vol. **56,** No.5, 815-822.

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

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* Vol.**40,** 1023-1028.

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

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

Hutchinson, S. (1997) *Computer crime in Canada* Unpublished Manuscript. In Rogers (2001) "Psychological Theories of Crime and "Hacking"" *http://www.escape.ca/~mkr/crime.doc*

Jordan, T. and Taylor, P. (1998) "A Sociology of Hackers" *The Sociological Review* Vol. **46, No.** 4, 757-780.

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

Malone, T.W. (1980) "What makes things fun to learn? A study of intrinsically motivating computer games" *Cognitive and Instructional Science Series* Vol. **CIS-7 SSL-80-11** Palo Alto, CA: Xerox

Malone, T.W. (1981) "Toward a theory of intrinsically motivated instruction" *Cognitive Science* Vol. **4**, 333-369.

Malone, T.W. & Lepper, M.R. (1987). "Making learning fun: A taxonomy of intrinsic motivations for learning". In R.E. Snow & M.J. Farr (Eds.), *Aptitude, learning, and instruction; III. Cognative and affective process analyses* (pp. 223-251) Hillsdale, NJ: Erlbaum.

Parker, D. (1998). *Fighting computer crime: A new framework for protecting information* New York: John Wiley & Sons, Inc.

Post, J. (1996). The dangerous information system insider: Psychological perspectives. *http://www.infowar.com/*

Rayport, J. F. & Jaworski, B. J. (2000) *e-Commerce* New York: McGraw-Hill.

Rogers, M. (1999) "Psychology of Hackers: Steps Toward a New Taxonomy" *Hacker Sitings and News* *http://www.infowar.com/hacker/99/HackerTaxonomy.shtml* 25/7/01.

Rogers, M. (2001) "Psychological Theories of Crime and "Hacking"" *http://www.escape.ca/~mkr/crime.doc*

Sterling, B. (1992) *The Hacker Crackdown: Law and disorder on the electronic frontier* Toronto: Bantam Books.

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

Taylor, P. (1998) *Hackers: the hawks and the doves-enemies & friends* Unpublished Manuscript. In Rogers, M. (2001) "Psychological Theories of Crime and "Hacking"" *http://www.escape.ca/~mkr/crime.doc*

Trevino,L.K. and Webster J. (1992). "Flow in computer-mediated communication: Electronic mail and voice mail evaluation and impacts" *Communication Research* Vol. **19**, 539-573.

Webster, J., Trevino, L.K. & Ryan, L. (1993) "The Dimensionality and Correlates of Flow in Human-Computer Interactions" *Computers in Human Behavior,* Vol. **9,** 411-426.

Webster, J. (1989) *Playfulness and computers at work* Unpublished doctoral dissertation, New York University

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

About the Author:

John Van Beveren; School of Business, University of Ballarat, University Drive, Mount Helen Victoria, Australia; Ph: +61 3 53 279 415; Fax: +61 3 53 279 405; E-Mail: j.vanbeveren@ballarat.edu.au

