Cybercrime Classification: A Motivational Model

Madison Ngafeeson

College of Business Administration
The University of Texas-Pan American
1201 West University Drive, Edinburg, Texas 78541, USA
Phone: (504)-810-3717
mnngafeeson@broncs.utpa.edu

ABSTRACT

As cybercrime continues to take up a disturbing publicity in the trends that mark our century, the commitment of governments, businesses and the global community to fight this pandemic is not surprising. However, combating this ill will entail identifying, defining and classifying cybercrime. Meanwhile the cybercrime phenomenon is now well known and defined; its classification has been limited at the top-level to a dichotomy of "computer-assisted" and "computer-focused" cybercrimes. This paper examines the crime theory and makes use of two primary motivation models plus four others to posit a motivational framework for cybercrime classification. The proposed model exposes a more holistic perspective on the topic, and would prove a useful tool for all the stakeholders in the battle against cybercrime.

Keywords: cybercrime; motivational model; classification

INTRODUCTION

Globalization, technology and the Internet are without a doubt shaping the way business is done today. While these phenomena are known to have brought global business to a whole new level, they have also brought with them, the mixed blessing called "cybercrime." Businesses, governments and individuals have all played victim to cybercrime. Many have attempted a definition of "cybercrime." Fafinski, & Minassian (2008) quoting Wall (2007), define cybercrime as "the transformation of criminal or harmful behavior by networked technology", while Wilson (2007) puts it simply as a "crime that is enabled by, or that targets computers". Other synonyms exist like "computer crime" and "internet crime", are also found in literature. Cybercrimes can range from criminal activity against data to content and copyright infringement (Gordon & Ford, 2006). The United Nations had this to say about efforts to fight crime in general.

> Globalization opens many opportunities for crime, and crime is rapidly becoming global, outpacing international cooperation to fight it…
>
> *United Nations Human Development Report, 1999*

Fighting cybercrime like any other crime requires three important elements namely: identification, classification and the actual deployment of effective counter-measures. Cybercrime has been clearly identified as a clear menace (Emigh, 2004) and fairly defined over the years (Gordon & Ford, 2006; Wilson, 2007; McCusker, 2007). However, the classification of cybercrime which is an important step to fighting it, has been grossly limited to whether these crimes are “computer-assisted” or “computer-focused” (Furnell, 2001) or simply by directly naming these crimes (Audit Commission, 1998). Only few, for example, Furnell (2001) attempted a classification based on a different view—motivation. However, his “categorizations of hackers” only addressed a small subset of cybercrimes, and never the whole.

We now turn our attention to major classifications of cybercrimes in available in literature. Furnell (2001) does a good job in reviewing past classifications as far back as twenty years into the categorizations put forth by the United Kingdom (UK) Audit Commission on computer crimes. Below are the categorizations and organization responsible for them as reviewed by Furnell.

UK Audit Commission (1998) Classification

- Fraud
- Theft
- Use of unlicensed software
- Private work
- Misuse of personal data
- Hacking
- Sabotage.
- Introducing pornographic material.
- Virus.

FBI’s National Crime Squad (Fraser, 1996)

- Intrusions of the Public Switched Network (the telephone company)
- Major computer network intrusions
- Network Integrity violations
- Industrial espionage
- Pirated computer software
- Other crimes where the computer is a major factor in committing the criminal offense

Computer Security Institute (CSI) (CSI, 2001)

- Theft and proprietary information
- Sabotage of data or networks
- Telecom eavesdropping
- System penetration by outsider
- Insider abuse of net access
- Financial fraud
- Denial of Service
- Spoofing
- Virus

- Unauthorized insider access
- Telecom fraud
- Active wiretapping
- Laptop theft

It was based on the above classifications that Furnell (2001) posited a model in which cybercrimes at a high level were classified simply as “computer-assisted” and “computer-focused” crimes.

Gordon and Ford (2006) also classified cybercrimes into two major group called “Type I” and “Type II” cybercrimes. This model, nevertheless, is similar to the Furnell (2001) classification for the simple fact that the former looked at cybercrime as a continuum ranging from crime which is almost entirely technological in nature to crime which really at its core was entirely people-related, hence, not differing from the view of cybercrime as either “computer-assisted” or “computer-focused.” In the case where these crimes were almost entirely technological, according to Gordon and Ford, it could be said that this would fit into the Furnell category of “computer-focused” crime while those that were nearly entirely people-related, could be considered in the category of “computer-assisted” crime. Whichever way we look at these classifications, it is clear that the classifications are closely related.

STATEMENT OF PROBLEM

As accessibility to the Internet grows, many people are becoming victims to cybercrime (Fafinski & Minassian, 2008). Technology and crime in recent history have known an unhealthy cohabitation. “Technology breeds crime. It always has, it always will,” said Frank Abagnale, the con-artist-turned-FBI-associate whose exploits were demonstrated in the Hollywood blockbuster “Catch Me If You Can” (Pereira, 2005). A research revealed that 90% of United States companies have been the target of a cyber attack, with 80% suffering a financial loss while UK businesses had at least one malicious in the previous year, double the number in 2000—averaging a loss of £30,000 per business and general loss in excess of £500,000 (Hinde, 2003). D’Ovidio (2007) quotes Cowan (2004) in graphic terms—“Cyber Crime Costs Business Billions”! There is no gainsaying that cybercrime “business” will continue to be a billions-of-dollar industry unless something is done, and quickly so.

It would seem obvious that combating cybercrime will take more than just the current efforts in force today. This, therefore, calls for a classification that exploits the very foundation of crime itself—motivation. Until crime is seen from the view of motivation for crime itself, efforts to battle it will not yield their full promise. Computer criminals are driven by time-honored motivations. Spotting these motivations and could be an essential key to finding a holistic solution. Not much research has looked into this important aspect of cybercrime classification. For example, Furnell (2001) discusses the subject of hackers and their motivation. In his work he highlights seven elements of motivation to wit: challenge, ego, espionage, ideology, mischief, money and revenge. Furnell then uses these motivational factors to distinguish nine types of hackers namely: “cyber-terrorists”, “cyber warriors”, “hacktivists”, “malware writers”, “phreakers”, “samurai”, “script kiddies”, and “warez d00dz”.

As plausible as these classifications may seem, they still fall short of helping governments, law enforcement specialists, businesses and the community at large as to explore the nature of these motivational factors and to use them to construct new proposition of cybercrime prevention as against mere cybercrime security. This paper delves into this subject in more detail in the following sections.

STATEMENT OF OBJECTIVE

This paper identifies the key determinants of crime, examines six key motivational theories and posits a motivational model for crime classification using two of these theories, while the remaining four theories are used to validate the model. Cybercrime is first and foremost a crime and hence, possesses the very fundamental "genetics" of traditional crime. These determinants of crime are discussed from the significant contribution of literature on conventional crime like those of Buonanno (2003), Brown (2001), Buettner and Spengler (2003), and Levitt and Lochner (2000). The theories used are Maslow's motivation theory (Maslow, 1954), Herzberg's motivation-hygiene theory (1959), Vroom's 1964 expectancy theory (as cited by Hunt & Hill, 1969), McGregor's (1960, 1967) X and Y theories, and finally, Ouchi's 1982 Z theory. While the Maslow and Herzberg models are used for the classification, the remaining models are used in the validating the proposed model.

Determinants of Crime and the Theories of Motivation

Cantor and Land (1985) restating Cohen and Felson (1979) said that the production of crime requires the presence of both (1) motivated offenders and (2) suitable targets (individuals or their property), in (3) the absence of effective guardians. What this means is that a crime is only possible when a motivated offender interacts with an ineffectively guarded target. Cantor and Land further argue that many conventional criminogenic theories (e.g. strain theory, utilitarian rational-choice theory, and conflict theory) are motivationally focused and therefore, take up as objective the identification of the forces that drive individuals toward criminal acts. But what exactly are the determinants of crime irrespective of medium—in this case, "the computer"?

Many streams of research have been carried out in this area. In Table 1 below, the work of several researchers are crystallized to point out the major determinants crime. As can be seen from the results, the determinants of crime can be classified into five major categories namely: social factors, economic factors, educational factors, biological factors, criminal justice system factors. Social factors refer to those factors that are related to the society and how it is generally organized (e.g. family structure). Economic factors are those that examine factors relating to or affecting material and financial resources. Educational factors touch issues of educational level of those involved in crime. Biological factors probe in race or gender. Lastly, criminal justice system factors refer to those factors as the law enforcement and punishment. Summarily, these factors contribute to whether or not someone gets involved in crime or not. A closer look at these determinants reveals that socio-economic factors are a dominant category.

Though these determinants are known to indicate an individual’s propensity to commit a crime, what truly makes them do it? This is a question of actual motivation. We proceed to discuss two key motivational theories use in this paper.

The Maslow Theory of Hierarchical Needs

Maslow in 1954 as summarized by Hunt and Hill (1969) hypothesized five broad classes of needs arranged in a hierarchical fashion such that when one level of need is met, the next level is automatically triggered. His five categories are: (1) physiological needs; (2) security or safety needs; (3) social, belonging or membership needs; (4) esteem needs; further sub-divided into self-esteem and esteem for others; and (5) self-actualization or self-fulfillment needs.

The Herzberg Motivation-Hygiene Theory

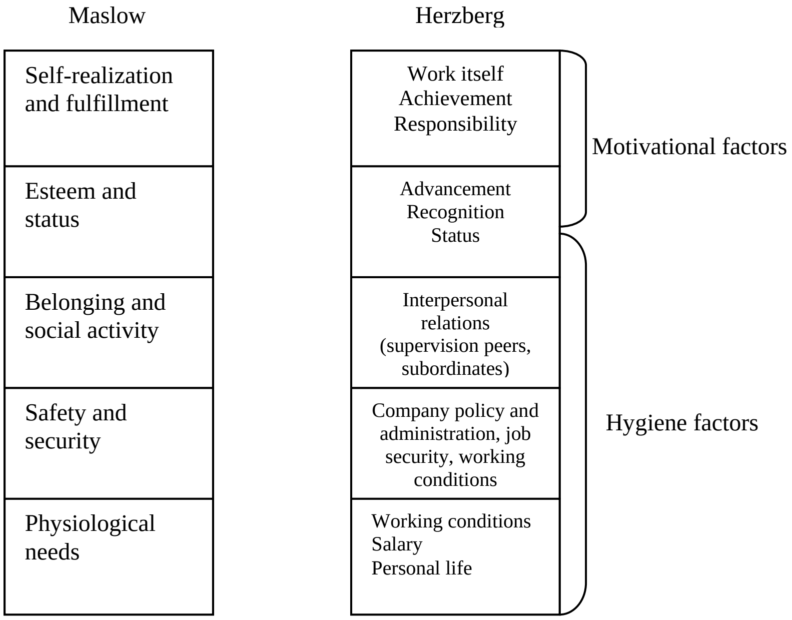
Herzberg and associates in 1959 proposed the two-factor theory popularly known as the *Motivation-hygiene theory*. The Herzberg model presents a dichotomy: “job content characteristics”—motivators responsible for satisfaction and “job environment characteristics”—hygiene responsible for dissatisfaction at work (Hunt & Hill 1969). The motivators include achievement, recognition, advancement, possibility of growth, responsibility, and work itself. *Hygienes*, on the other hand include salary; interpersonal relations with superiors, subordinates, and peers; technical supervision; company policy and administration; personal life; working conditions; status; and job security. In Figure 1 below, it is shown how the Maslow and Herzberg models relate in conveying the notion of motivation. There exist some degree of overlap in categories in the models; however, the idea here is to show how both theories “agree” with each other.

Summarily, while it is that “traditional crime” is different from “cybercrime”, they both share a common denominator—“crime”; hence, the determinants and motivational factors of both conventional crime and cybercrime would be the same since they only differ in the medium in each case. Furthermore, in evaluating the motivation of cybercriminals, it is safe to predict that criminal action will be motivated by “need” (Maslow model) or by “work content/environment characteristics” (Herzberg model). This idea is corroborated by the findings of the researchers stated earlier to identify the determinants of crime (Buonanno, 2003; Buettner & Spengler, 2003; Cantor & Land, 1985; and Levitt & Lochner, 2000).

Table 1: Crime determinants

Reference	Determinants
Buonanno, 2003	- Differential wages
	- Income level
	- Probability of arrest / punishment
	- Level of education / non-education
	- Social interactions
	- Age
Buettner & Spengler, 2003	- Unemployment
	- Poverty
	- Inequality
	- Mobility (non-resident criminals)
Cantor & Land, 1985	- Unemployment
Brown, 2001	- Lower incomes
	- Higher unemployment
	- Lower educational achievement
	- Socio-cultural status
Levitt & Lochner, 2000	- Biological
	- Social
	- Criminal justice system
	- Economic factors

Figure 1: Need-Priority (Maslow) model versus Motivation-Hygeine (Herzberg) model



Adapted from Hunt and Hill (1969)

It would be useful at this point to acknowledge a research work that attempted to cybercrime classification from a motivational framework standpoint. Furnell’s (2001) work was limited to “hackers and their motivation” as stated by the author. Though he suggested that this type of classification could be applied to other classes of cybercrime, he did not exactly say how. Furnell first of all classified hackers at the top level to be divided into “Black hat”, “White hat” or “Grey hat” hackers based on motivation. Black Hat hackers referred to the majority of hackers—those whose intrusion into the system is clearly unauthorized and frequently malicious—also referred to as “dark side” hackers. White Hats, on the other hand are “ethical” hackers working for the good of system security. Grey Hats was used to describe a third group which is in between the previous two—hackers whose intentions were unclear and could change. At the lower level, he classified hackers into eight categories as in the Table 2 below. He then characterized these types of hackers according to their motivation. Since the purpose for this portion of this paper is to point to underscore the motivational aspects he highlights, no attempt has been made to define the hacker categories he used namely: Cyberterrorists, Cyber Warriors, Hactivists, Malware Writers, Phreakers, Samurai, Script Kiddies, and Warez D00dz. The motivational categories used to classify aforementioned types of hackers are: challenge, ego, espionage, ideology, mischief, money and revenge. These categories can be incorporated into the Maslow-Herzberg model very well but not the contrary. Hence, showing the Maslow-Herzberg model a more holistic and explanatory model.

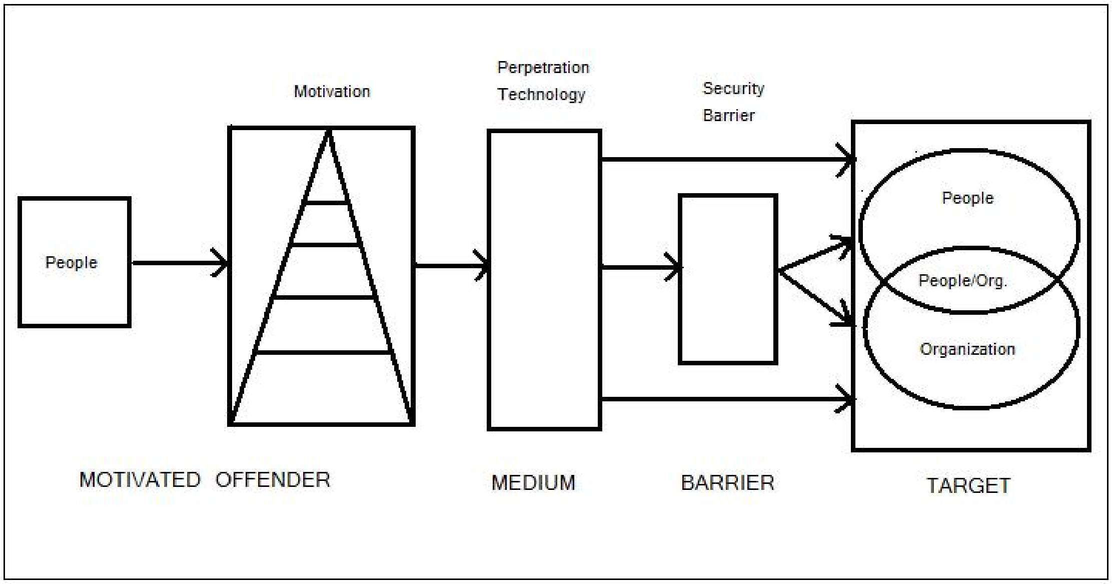
Table 2: Hackers and their motivations (Furnell, 2001)

	Cyber-terrorists	Cyber Warriors	Hacktivists	Malware writers	Old School	Phreakers	Samurai	Script kiddies	Warez D00dz
Challenge				✓	✓	✓	✓		✓
Ego				✓	✓	✓			✓
Espionage		✓		✓					
Ideology	✓	✓	✓		✓				✓
Mischief				✓		✓		✓	
Money		✓		✓		✓	✓		✓
Revenge	✓		✓	✓				✓	

THE MOTIVATIONAL MODEL OF CYBERCRIME

The motivational model of cybercrime in Figure 2 below combines three theoretical frameworks: Maslow’s theory of hierarchical needs (Maslow, 1954); Herzberg’s 1959 two-factor theory (Hunt & Hill, 1969); and the 1979 work of Cohen and Felson on how crime elaborating the steps involved in the production of crime (Cantor & Land, 1985).

Figure 2: The Motivational Model of Cybercrime Classification



A general look at the model of the model reveals a motivated offender who uses the medium of technology to attack a target. According to Cohen's and Felson's 1979 crime production model (Cantor & Land, 1985), the motivated offender will produce a crime i.e. attack his target in the absence of effective guardians. What this means is that a motivated cybercriminal who uses technology can attack a particular target either by profiting from a complete lack of defense, or from a weak defense, or better still by overpowering the barrier. At a general level, this model is very similar to a typical security model where people trying to access a company or business network are passed through an initial firewall to access the company's local area network (LAN), but if they will need to access company's restricted database systems or servers, they will need to break through another firewall(s) to access it. The motivational model of cybercrime; therefore, perfectly blends with the generals of a typical security model.

Motivational model components

People

People refer to potential offenders or criminals. When *people* are exposed to one or more of the determinants of crime discussed earlier, they may become motivated to carry out a particular behavior. Without the presence of these predisposing factors, some people may only stay as latent potential candidates and may never really get to commit a cybercrime.

Motivation

This component refers to the various factors that "push" *people* to carry out cybercrime. First, they are triggered by the determinants of crime for example, unemployment, low median income, poverty, wage inequality, social status etc. (Buonanno, 2003); driven by the desire to fulfill or satisfy "needs", they then indulge into the act. These needs as elaborated by the Maslow-

Herzberg model described previously, range from (1) “physiological needs”; (2) “safety needs”; (3) “belonging needs”; (4) “esteem needs” and (5) “self-actualization needs”. As the Maslow model hypothesizes, as we move up the hierarchy of needs, satisfaction and fulfillment is increases. This implies that the propensity for crime is higher among those who have more “basic” needs to fulfill than for those at the tip of the pyramid (the self-actualized). Efforts to fight crime for instance, may involve seeking for some of these basic needs and meeting them to “kill” or curb the motivation and propensity for criminal actions.

Brown (2001) argues that in order to decide whether to commit a crime or not, a cost-benefit analysis is undertaken by the individual. Hence, the cost of criminal activity must be considered. Four types of costs are considered by the criminal as set forth by Brown. Firstly, direct costs involved in committing the crime. These involve the skills, equipment and contacts needed for the crime. Second, the punishment costs are also considered. The expected punishment costs therefore depend not only on the nature and size of punishment, but also on the probability of being caught or arrested. Third, opportunity costs are considered too. This means that the net estimated benefits of committing crime are compared with those of a legal employment. If the net benefits exceed zero or are more, the criminal is likely to consider the crime option. For this reason, underemployment and unemployment are obvious risk factors that easily cause the cost-benefit of the criminal to tip to a net benefit, and hence the higher probability to commit a crime. Fourthly, there is a moral cost involved. Though economists often do not add this into the equation for reason of the difficulty to measure it; it still is important. Moral costs involve the cost of reputation and shame if cost. Summarily, the criminal weighs up expected costs and benefits of criminal activity and proceed to make a choice to engage in activity if net benefits generally are positive or exceed zero.

With falling transaction costs in internet and computer technologies (Bakos, 1998), the high probability to remain anonymous after committing a cybercrime, the advantage of not-so-defined legislation and jurisdiction (Pocar, 2004), cybercriminals may only be left with a moral cost to consider. Looking back to the Maslow-Herzberg model, the propensity to commit cybercrime is likely to reduce as we go up the pyramid given the foregone argument. Only self-actualizers care about fame, status, and reputation. Individuals on the base of the pyramid care about more practical and “tangible” needs. To mention the Herzberg two-factor model, the only group of individuals who fit into “motivator-factor” from the Maslow model is the self-actualizers; hence, strongly suggesting that levels of satisfaction/need can possibly predict criminal intention. In conclusion, cybercrimes can be classified into five major motivational classes therefore, corresponding to each class of need. This paper does not seek to propose the exact nomenclature, as it seeks to demonstrate the essence and importance of this motivational view. Once the motivation-factor is established, a perpetration technology is then chosen.

Perpetration Technology

This component refers to all technologies used to carry out cybercrime. These include but are not limited to computers, cell phones, disc drives, etc.—in short, hardware and software that can prove useful. The perpetration technology is then used to attack a target which could be a person, or an organization, or both. This attack may either be screened by a security barrier or not, depending on the situation. In the case where it is screened, the attack may either be successful—attaining the target, or unsuccessfully aborted.

Security Barrier
This component is comprised of hardware and software technological defenses (e.g. firewalls, anti-virus software, etc.); physical defenses (e.g. buildings that provide physical security); criminal justice system (by government); and educational defenses (protection through knowledge). These security barriers could be strong enough to protect the target, or may be overpowered by the attack so that the target is reached.

Target
The last component of the model is the target. This refers to the people or organization that is being targeted or both. The target is reached either through weak defenses or no defense at all. The targets (*people* and *organization*) also include the technologies they use. Most of the taxonomic schemes for cybercrime thus far (as discussed earlier) have concentrated around this area—presenting a high level classification that consists of dichotomy of "computer-assisted" cybercrimes on one end, and "computer-focused" cybercrime on the other. The *target* therefore, represents the "damages-end" of the model. At this level, people and organization are left to deal with the woes of cybercrime.

CONCLUSIONS AND IMPLICATIONS

In a global environment plagued by an ever-growing community of ill-intentioned cybercriminals whose deleterious effects are obvious on affected people and organizations, every contribution to a fuller and more comprehensive understanding of the determinants and components, and how these components relate is critical. This paper synthesized major cybercrime determinants viz. differential or inequality in wages, low income levels, unemployment, educational level, social interactions, the criminal justice system and biological determinants to show how each of these help to explain the motivation for cybercrime.

Six motivational theories are brought together to examine cybercrime from a motivational perspective. While the Maslow and Herzberg models are compared and both used build the motivational model of cybercrime classification, the Vroom, McGregor, and Ouchi models are used to validate the proposed model. Apart from few works like that of Furnell's (2001), most previous works dwelt on the classification system that relied on a top-level dichotomy that viewed cybercrime as "computer-focused" or "computer-assisted."

The proposed model-built is quite similar to a typical security model, is composed of five major components to wit: people, motivation, perpetration technology, security barrier and the target. The robust nature of the model makes it to incorporate the motivational dimension as a beginning component, while the previous classification is incorporated in the last component.

This work would prove useful in contributing to a more holistic perspective on cybercrime classification. This view of the evil of cybercrime would benefit legal professionals as well as governments in their efforts to fight cybercrime by formulating a whole new proposition of "cybercrime prevention" and not just "cybercrime security." While it is true that we need to be "firewalled" against cybercrime, it would make sense to address the very reason why cybercriminals do what they do in the first place. Even though the proposed model focuses on motivational classification, it still shows how the other classifications fit into the overall model, proving it robustness. This model would serve as a tool for legal professionals, legislators and governments by presenting a framework for an integrated approach to cybercrime-combat.

LIMITATIONS AND DIRECTIONS OF FUTURE STUDIES

Though this model is theoretically validated and assessed, it would be good for empirical testing to be carried out using it to see how practical it can be, and possible modifications be proposed. The model looked at cybercrime from a purely motivational standpoint. It is possible that other perspectives will point to a better and more comprehensive model.

REFERENCES

Audal, J., Lu, Q., & Roman, P. (2008). Computer Crimes. *The American Criminal Law Review, 45(2),* 233-274.

Bakos, Y. (1998, August). Emerging Role of Electronic Marketplaces on the Internet. *Communications of the ACM, 41(8),* 35-42.

Balfour, D. L. & Marini, F. (1991). Child and Adult, X and Y: Reflections on the Process of Public Administration Education. *The American Society of Public Administration, 51(6),* 478-485.

Brown, K. V. (2001, June). The Determinants of Crime in South Africa. *The South African Journal of Economics, 69(2),* 269-298.

Buettner, T., & Spengler, H. (2003). Local Crime Determinants: Distinguishing Between Resident and Non-resident Offenders. *Darmstadt Discussion Papers in Economics, 120.*

Buonanno, P. (2006). The Socioeconomic Determinants of Crime: A Review of the Literature. *University of Milan-Bicocca, Working Paper Series, 63.*

Cantor, D. & Land, K.C. (1985, June). Unemployment Rates and Post-World War II United States: A Theoretical and Empirical Analysis. *American Psychological Review, 50(3),* 317-332.

D'Ovidio, R. (2007). The Evolution of Computers and Crime: Complicating Security Practice. *Security Journal, 20,* 45-49.

Emigh, J. (2004). Cybercrime Can Have Real-World Ramifications. *Access Control Security Systems, 47(1),* 36-37.

Fafinski, S. & Minassian, N. (2008, June). *UK Cybercrime Report 2008.* New York: Garlik.

Furnell, S. M. (2001). The Problem of Categorising Cybercrime and Cybercriminals. *2nd Australian Information Warfare and Security Conference 2001.*

Gordon, S. & Ford, R. (2006). On the Definition and classification of Cybercrime. *Journal of Computer Virology.* 2:13-20.

Hinde, S. (2003). The Law, Cybercrime, Risk Assessment, and Cyber Protection. *Computers and Security, 22(2),* 90-95.

Hunt, J.G. & Hill, J. W. (1969). The New Look in Motivation Theory for Organizational Research. *Human Organization, 28(2),* 100-109.

Levitt, S. D. & Lochner, L. (2000). *The Determinants of Juvenile Crime. (in Jonathan Gruber, ed., Risky Behavior Among Youths: An Economic Analysis)* Chicago: University of Chicago Press, 327-73.

Markwell, J. (2004). The Humaan Side of Schience Education: Using McGregor's Theory As a Framework for Improving Student Motivation. *Biochemistry and Molecular Biology Education, 32(5),* 323-325.

Maslow, A. H. (1954). *Motivation and Personality.* New York: Harper and Row.

McCusker, R. (2006). Transnational Organised Crime: Distinguishing Threat from Reality. *Crime Law and Social Change, 46,* 257-273.

Miner, J. B. (1984, April). The Validity and Usefulness of Theories in an Emerging Organizational Science. *The Academy of Management Review, 9(2),* 296-306.

Pereira, P., (2005, September). Double-Edged Security: Technology and Crime are uneasy partners. *eWeek, 22*(37), C6-C7. Retrieved October 17, 2007, from Sciences Module database. (Document ID: 906452121)

Pocar, F. (2004). New Challenges for International Rules against Cyber-crimes. *European Journal on Criminal Policy and Research, 10(1)*, 27-37.

U.S. Department of Justice (2004, March). *Cybercrime against Businesses.* (Bureau of Justice Statistics Report NCJ 200639).

UN Office of Drugs and Crime. (2007). "Assessment of Transnational Organized Crime in Central Asia."

Wilson, C., (2007). Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. *Congressional Research Service.*