2014

A Cybercrime Taxonomy: Case of the Jamaican Jurisdiction

Charlette Donalds
The University of the West Indies, charlette.donalds02@uwimona.edu.jm

Kweku-Muata Osei-Bryson
Virginia Commonwealth University, kmuata@isy.vcu.edu

25P. A Cybercrime Taxonomy: Case of the Jamaican Jurisdiction

Charlette Donalds
The University of the West Indies,
charlette.donalds02@uwimona.edu.jm

Osei-Bryson, Kweku-Muata
Virginia Commonwealth University
Kmuata@ISY.VCU.Edu

Abstract

Cybercrimes over the years have become both increasingly numerous and sophisticated. This paper presents a taxonomy for cybercrimes that can be used for the analysis and categorization of such crimes, as well as providing consistency in language when describing cybercrimes. This taxonomy is designed to be useful to information bodies such as the Jamaican Cybercrime Unit, who have to handle and categorize an ever increasing number of cybercrimes on a daily basis. Additionally, cybercrime investigators could use the taxonomy to communicate more effectively as the taxonomy would provide a common classification scheme. The proposed taxonomy uses the concept of characteristics structure. That is, the taxonomy classifies properties about that which is being classified and not by the object itself. The taxonomy consists of characteristics which provide a holistic taxonomy in order to deal with inherent problems in the cybercrime field.

Keywords

Cybercrime, Taxonomy, Classification, Jamaica

1. Introduction

In recent times police investigators attached to the Cybercrime Unit[1] (CU) in the Jamaica Constabulary Force (JCF) are cautioning citizens about protecting personal information and to be prudent about what is placed on digital media and the Internet, because they claim, cyber-related crimes are on the increase (see, for example, Reynolds-Baker, 2012). Further, investigators claim that in recent years cyber-related crimes are evolving to include such offences as cyber defamation, unauthorized access, impersonation, obscene publication, denial of service, cyber espionage, hacking for financial gain (Henry, 2009; Reynolds-Baker, 2012) and lottery scamming (Associated Press, 2012).

Perhaps the claims about the growth and trending of cybercrimes are legitimate; however, the true extent of different types and trending of cybercrimes in Jamaica is currently unknown. In fact, a review of the literature reveals mostly information from the trade press about prominent cybercrime incidents occurring in Jamaica. And while these cybercrimes are discussed qualitatively, there are no commensurate attempts at quantitative or analytical investigations of these and other cybercrimes. Reliable data and empirical analyses of cybercrimes are important,

[1] The full name of this unit is Communication Forensic and Cybercrime Unit.

however. These elements are prerequisites for the advancement of critical knowledge on which effective cybercrime investigative strategies and legislative measures are to be developed.

To address this gap and to advance knowledge about the different types and trending of cybercrimes, we attempted to quantitatively explore cybercrimes reported between 2010 and 2011 to the CU. It was then that the need for a comprehensive cybercrime taxonomy arose. Although several lists of terms or categories of cybercrimes are proposed, when we applied them to our data they were inadequate for several reasons: 1) since new cybercrimes frequently appear, they tend to be incomplete; 2) terms tend not to be mutually exclusive and an actual cybercrime could be classified under multiple headings; 3) categories tend to be too broad to be useful in disaggregating cybercrimes; and 4) classification of cybercrimes tend not to be repeatable (depending on who was classifying, the same cybercrime could be placed under different categories). Further, there is still no single established cybercrime taxonomy in general use. According to Moitra (2004, p. 110), "one outstanding problem in cybercrime is the development of a suitable, comprehensive taxonomy for criminals, crimes, and the impact of the crimes". Therefore, we decided to develop a cybercrime taxonomy that can be used to analyze our data as well as be useful to others.

The definition of and properties of a sufficient and acceptable taxonomy are discussed in Section 2. In Section 3 we first present an overview of existing cybercrime and computer and network security taxonomies followed by an evaluation of these taxonomies based on properties of a sufficient and acceptable taxonomy. In the next section a brief outline of the design approach is outlined followed by the taxonomic characteristics of the proposed taxonomy. Section 5 concludes with key points presented in the paper and next steps in the research.

2. Taxonomy

Taxonomies establish organizing frameworks, essential for the development of a field. According to Glass and Vessey (1995, p. 65) "without an organizing framework, researchers and practitioners find it hard to generalize, communicate, and apply research findings. Taxonomies structure or organize the body of knowledge that constitutes a field, with all the potential advantages that brings for the advancement of the field". According to Clinard et al. (1994), taxonomies are regarded as a necessary stage in the development of a specific theory. They further state that taxonomies "not only reduce phenomena to more systematic observation, they also assist in the formulation of hypotheses and serve as guides for research" (Clinard et al., 1994, p. 2). Tittle and Paternoster (2000) concur in stating that the classification of individual instances into similar abstract types (a taxonomy) brings order to a seemingly disparate phenomena and might suggest underlying principles that could simplify the obvious complexities of the subject matter. Therefore, what is a taxonomy? In this study it is defined as "a classification system where the classification scheme conforms to a systematic arrangement into groups or categories according to established criteria" (Undercoffer, Pinkston, Joshi, & Finin, 2003, p. 2). The creation of a taxonomy with classification categories is therefore an important and necessary prerequisite for systematic study (Howard & Longstaff, 1998). Nowhere is this truer than for the study cybercrime.

A cybercrime taxonomy is beneficial for several reasons: 1) it enables the compilation of cybercrime statistics, from which patterns and trends can be observed and other conclusions

inferred. Additionally, identifying patterns and trends can offer predictive capabilities and isolate and discount popular misperceptions and misrepresentations of cybercrime issues (Walden, 2007); 2) it enables more robust, complete and comprehensive data collection when incidents are reported to investigators, such as to those in the CU. (Currently, only basic data about cybercrime incidents are captured by CU investigators. Incidents are grouped based on list of incident categories, however, this does not constitute a proper taxonomy as it co-mingles outcome, offence, intent and technique in an informal manner.); 3) it can improve information sharing between cybercrime stakeholders within and between countries (Land, Smith, & Pang, 2013); 4) it can be used as a basis for improving education and raising awareness (Furnell, 2001); and 5) it enables better allocation of resources to combat cybercrimes at organizational, national and international levels (Land et al., 2013).

2.1 Properties of a Taxonomy

In this section we propose requisite properties of a sufficient and acceptable taxonomy for cybercrime. While a review of the literature does not reveal requisite properties for taxonomies in the cybercrime domain, it reveals sufficient and acceptable properties for taxonomies in the computer and network security domain. These characteristics are adapted to the cybercrime domain since both domains, among other things, focus on crime and other illicit activities that involve the use of networked technologies. The following properties are identified as essential to a cybercrime taxonomy:

- ***Mutually Exclusive*** (Amoroso, 1994; Howard, 1997; Hunton, 2009; Lindqvist & Jonsson, 1997; Undercoffer et al., 2003): each cybercrime should fit in at most one category in the taxonomy.
- ***Complete/Exhaustive*** (Amoroso, 1994; Howard, 1997; Lindqvist & Jonsson, 1997; Undercoffer et al., 2003): taken together, the categories should account for all cybercrimes. Perhaps it will be difficult to prove a taxonomy complete or exhaustive, however, it can be justified through successful categorization of actual cybercrimes.
- ***Comprehensible*** (Lindqvist & Jonsson, 1997): the taxonomy should be understood by those who are in the cybercrime field, as well as those who only have an interest in it.
- ***Established Terminology*** (Lindqvist & Jonsson, 1997): existing terminology should be used in the taxonomy so as to avoid confusion and to build on previous knowledge.
- ***Repeatable*** (Amoroso, 1994; Howard, 1997; Krsul, 1998; Lindqvist & Jonsson, 1997; Undercoffer et al., 2003): regardless of who classifies, repeated applications should result in the same classification.
- ***Unambiguous*** (Amoroso, 1994; Howard, 1997; Lindqvist & Jonsson, 1997; Undercoffer et al., 2003): each category must be clearly defined and clear criteria should be specified for defining what cybercrimes are placed in each category in the taxonomy.
- ***Useful*** (Amoroso, 1994; Howard, 1997; Lindqvist & Jonsson, 1997; Undercoffer et al., 2003): the taxonomy could be used to gain insight into the cybercrime domain.
- ***Accepted*** (Amoroso, 1994; Howard, 1997; Undercoffer et al., 2003): the taxonomy should be logical and intuitive so that it can become generally approved or the accepted standard.

When developing the proposed cybercrime taxonomy, we considered these properties. Although it is reasonable to expect that a taxonomy satisfies all the properties identified above, researchers suggest that a satisfactory taxonomy may be limited in some of these characteristics (Hansman &

Hunt, 2005; Howard, 1997). Despite this suggestion, the objective of the proposed taxonomy is to satisfy all requisite properties.

3. Existing Taxonomies and Previous Work

In the fields of cybercrime and computer and network security, several taxonomies for classifying computer and high tech crimes, security threats and cybercrimes have been presented. In this section we review and evaluate some of the most prominent taxonomies. Some authors present computer and security taxonomies as lists of single terms. For instance, Cohen (1997) presents a list of 96 terms of potential attacks. However, lists are inadequate for several reasons. They generally fail to satisfy the requirements of a good taxonomy. For example, they tend to be incomplete (new attacks appear frequently) and terms tend not to be mutually exclusive (actual attacks can be located under multiple headings). Such taxonomies are omitted from the review.

Focusing on the role technology plays in the commission of the crime, an early attempt at a taxonomy of technological crimes, Carter (1995) considered four categories: 1) crimes in which the computer is the target; 2) crimes in which the computer is the instrumentality of the crime – instrumentality refers to the diversion of a lawfully possessed item, that is, an instrument, to facilitate committing a crime; 3) crimes in which the computer is incidental to other crimes such as money laundering; and, 4) crimes which are associated with the prevalence of computers, e.g., violation of copyright. Using the same underlying principle for classification, (i.e., the role technology plays), many other authors in the field present similar classification categories as Carter's. Table 1 summarizes these and other taxonomies that use different underlying principles for their classifications. Existing taxonomies are inadequate for several reasons: 1) classifying cybercrimes into few broad categories do not reduce the phenomena to more systematic observation; 2) relationships that may exist between dimensions/categories are not easily identified; 3) they do not satisfy some requisite properties proposed for a sufficient and acceptable cybercrime taxonomy, for instance, completeness (important dimensions are omitted), useful (when applied, cybercrime investigators would not gain insights), mutually exclusive and repeatable (the same cybercrime may be classified under multiple categories). Table 2 provides a summary evaluation of existing and the proposed cybercrime taxonomies against requisite properties for a sufficient and acceptable taxonomy. In Table 2 note: TBD = to be determine.

Despite the limitations of existing taxonomies, some provide useful approaches that are incorporated into the current work. For instance, Moitra (2004) distinguishes between cybercriminals, the crime and victim. Further, Howard (1997) identifies attackers, tools, access, results and objective as important dimension for classifying Internet security incidents. The taxonomies presented by Moitra (2004) and Howard (1997) are interesting as they appear to be well-founded and better suited for a more flexible and robust taxonomy for cybercrime that is invariant with respect to changing conditions and evolving technology.

4. Towards a New Taxonomy

A taxonomy may be created either *a priori* or *a posteriori*. An *a priori* taxonomy is created non-empirically whereas an *a posteriori* taxonomy is created by empirical evidence derived from some data set. The taxonomy proposed in this paper utilizes the *a priori* approach. However, in

the next phase of this project, we intend to use the *a posteriori* approach to revise the taxonomy as necessary.

Underlying Principle	Reference	Categories/Dimensions
Role technology plays in the commission of the crime	Carter (1995)	• Crimes in which computer is the target • Crimes in which the computer is the instrumentality of the crime • Crimes in which the computer is incidental to other crimes • Crimes which are associated with the prevalence of computers
	Smith et al. (2004) and Brenner (2010)	• Crimes in which a computer is the target • Crimes in which a computer is used as a tool • Crimes in which a computer plays an incidental/ancillary role
	Canadian Centre for Justice Statistics (CCJS) (2002)	• Crimes in which the computer is the tool • Crimes in which the computer is the object
	Urbas and Choo (2008)	• Crimes in which the technology is the target • Crimes in which the technology is the tool used
	Furnell (2001)	• Computer-assisted crimes • Computer-focused crimes
	Gordon and Ford (2006)	• Type I cybercrimes – crimes which are almost entirely technological in nature • Type II cybercrimes – crimes which are really, at their core, entirely people related
	Alkaabi et al. (2010)	• Type I cybercrimes – the computer is the target • Type II cybercrimes – the computer is the tool
Harmful behaviours	Wall (2001)	• Cybertrespass – unauthorized crossing of invisible yet salient boundaries of ownership online, primarily by hackers • Cyberdeception/theft – types of acquisitive harm possible in cyberspace • Cyberpornography/obscenity – publication or trading of sexually expressive materials online • Cyberviolence – distribution of injurious, hurtful or dangerous materials online
Nature of the cybercrime	Moitra (2004)	• The criminal – intent and actions of • The crime – kind and how committed • The victim – impact on
Entire attack process	Howard (1997)	Attackers → Tools → Access → Results → Objective

Table 1: Existing Taxonomies

4.1 Taxonomy Design Approach

The proposed taxonomy uses the concept of characteristics structure. Lough (2001, p. 152) defines a taxonomy with a characteristics structure as a "taxonomy with a set of categories consisting of different types of characteristics of that which is being defined." In other words, the taxonomy classifies properties about that which is being classified and not by the object itself. Characteristics are also called features or attributes and are the properties of the object to be classified (Krsul, 1998). According to Lough (2001), this type of taxonomic structure is analogous to the nucleotides (adenine (A), thymine (T), cytosine (C) and guanine (G)) of deoxyribonucleic acid (DNA) in that one or more of the characteristics of the taxonomy can be linked together to describe the item that is being placed in a taxonomy. This approach is used in the computer security domain. For instance, Lough (2001) proposes a taxonomy with a characteristics structure for software vulnerabilities consisting of four characteristics: Validation, Exposure, Randomness and Deallocation. Developing a taxonomy with a characteristic structure permits the characterizing of any cybercrime without regard for changing conditions and

evolving technology, important for the field of cybercrime given the rapidly changing technology.

Study	Mutually Exclusive	Complete/ Exhaustive	Comprehensible	Established Terminology	Repeatable	Unambiguous	Useful	Accepted
Carter (1995)	X	X	✓	X	X	✓	X	X
Smith et al. (2004); Brenner (2010)	X	X	✓	✓	X	✓	X	X
Furnell (2001)	X	X	✓	✓	X	✓	X	X
CCJS (2002)	X	X	✓	✓	X	✓	X	X
Gordon and Ford (2006)	X	X	✓	✓	X	✓	X	X
Urbas and Choo (2008)	X	X	✓	✓	X	✓	X	X
Alkaabi et al. (2010)	X	X	✓	✓	X	X	X	X
Wall (2001)	✓	X	✓	✓	X	X	X	X
Moitra (2004)	X	X	✓	✓	X	X	X	X
Howard (1997)	X	X	✓	X	X	X	✓	✓
Donalds and Osei-Bryson (this study)	✓	TBD	✓	✓	TBD	✓	TBD	TBD

Table 2: Taxonomy Evaluation by Requisite Properties

4.2 Taxonomy Characteristics

Our cybercrime taxonomy proposes nine characteristics: Victim, Attacker, Objective, Tool & Tactic, Impact, Result, Relationship, Target and Offence. These are discussed next.

4.2.1 Victim

A victim of a cybercrime is an entity that suffers harm, in relation to the cybercrime. A victim may be an individual, group, organization, government or country. A victim of a cybercrime may or may not be the same as the target.

4.2.2 Attacker

An attacker is defined as anyone who attempts one or more cybercrimes in order to achieve an objective (adapted from Howard & Longstaff, 1998). Authors categorize attackers based on differing principal components. For instance, some by threat properties (HaId & Pedersen, 2012); whether the attacker is internal vs. external to the entity attacked (Russell & Gangemi, 1991); still others by motivation (Furnell, 2001; Howard, 1997) or by motivation and knowledge

or skill level (Pfleeger, 1997; Rogers, 2006) or motivation, skill level, maliciousness and method used (Meyers, Powers, & Faissol, 2009).

A two-step approach is used in developing the attacker categories. First, we extend and/or combine existing categories to reflect the most current terminologies used for attackers in that category. Next, we add new categories that now cover cybercrime attackers that were previously ignored. Based primarily on the principal component motivation, each category is now described:

- ***Corporate Raiders*** – employees, business partners or agents/associates of nation states who infiltrate competitors' or other governments' networks, computers and/or systems to steal intellectual property or digitally stored proprietary information for financial gain.
- ***Hacktivists, Political Activists*** – use their technical skills to divert and bypass security systems in order to further their political agendas (Chopitea, 2012) and/or use the Internet as a tool for political change.
- ***Script Kiddies, Newbies, Novices*** – have limited computer and programming skills, are usually new to hacking and use pre-written software, referred to as toolkits, in their exploits and are motivated out of personal satisfaction such as thrill-seeking, ego stroking, curiosity and boredom (Meyers et al., 2009; Rogers, 2006).
- ***Cyber-punks, Coders, Writers*** – have better computer skills, programming capabilities and a better understanding of the systems they attack, write some of their own scripts and engage in malicious acts to gain media attention, prestige and notoriety (HaId & Pedersen, 2012; Meyers et al., 2009; Rogers, 2006).
- ***Insiders, User Malcontents*** – current or former disgruntled employees or contractors who intentionally exceed or misuse an authorized level of network, system or data access in a manner that affects the security of the organizations' data, systems, network or daily business operations (Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2004) and are most frequently motivated by revenge (Kowalksi, Cappelli, & Moore, 2008).
- ***White Hat Hackers, Old Guard, Sneakers*** – primarily motivated by curiosity and the intellectual challenge of beating the security system, they appear to have no criminal or malicious intent, even though they often show a lack of regard for personal privacy (Meyers et al., 2009; Rogers, 2006).
- ***Black Hat Hackers, Professionals, Elites*** – professional criminals, motivated by money and financial gain, who put their technical skills and ability to use in furtherance of their criminal enterprise (Meyers et al., 2009; Rogers, 2006).
- ***Cyber Terrorists, Cyber Warriors, Information Warriors*** – highly trained, highly skilled attackers, motivated by politics or ideology, and who conduct attacks that destabilize, disrupt, and destroy the cyber assets and data of an enemy nation or government organization (Furnell, 2001; Meyers et al., 2009; Rogers, 2006).
- ***Digital Pirates, Copyright Infringers*** – individuals who obtain unauthorized use or possession of, engage in unauthorized duplicating, distributing, downloading, displaying or sale of copyrighted digital material for the purpose of commercial advantage, private financial gain or for self-aggrandizement.
- ***Online Sex Offenders, Cyber Predators, Pedophiles*** – attackers in this category uses the Internet to exploit, or take advantage of, or engage in sexual deviant behavior with children. The main motive is sex or other forms of abuse.

4.2.3 Objective

Objective is related to the attacker and is defined as the main purpose or end goal of a cybercrime (adapted from Howard & Longstaff, 1998). A variety of objectives have been identified why technology crimes and cybercrimes are committed. Collectively, authors identify: challenge, status, thrill; political gain; financial gain; revenge; politics, ideological; and sexual impulses (Choo, Smith, & McCusker, 2007; Howard & Longstaff, 1998; Moitra, 2004; Shinder, 2003). The following categories of objective are proposed:

- ***Curiosity, Challenge, Thrill –*** attackers who are driven by boredom or curiosity and by the thrill of gaining knowledge and beating the system.
- ***Status, Fame-seeking, Self-aggrandizement*** – attackers who seek out fame for committing malicious acts.
- ***Financial Gain*** – attackers who make financial profit from their crimes.
- ***Anger, Revenge*** – attackers who believe great torts have been done to them or someone they care about, be it real or perceived.
- ***Political, Ideological*** – attackers who fight for what they believe to be legitimate issues and who are intent on creating damage or disruption to nations or organizations opposed to their causes or beliefs.
- ***Sexual Impulses*** – attackers whose sexual behavior is considered inappropriate, harmful or illegal. Child pornographers who may exploit the sexual impulses of others for profit would not fit in this category; instead, their motivation is monetary and they would therefore fit in the *financial gain* category.

4.2.4 Tool & Tactic

Tool and tactic are means of committing cybercrimes. They are representations of the behavior or *modus operandi* of the attacker. Tools and tactic are classified as follows:

- ***Tool*** – hardware or software used by an attacker to achieve the objective. Examples of tools include packet sniffer/injectors, password generators, key loggers and card readers.
- ***Attack Vector*** – "a term used to describe a method that delivers a payload to a target device without consent and with the intention of using the technology for an undesirable or illicit purpose" (Hunton, 2009, p. 532). Common attack vectors include viruses, worms, malware, DoS and spybots.
- ***Social Engineering*** – a term used to describe the use of psychological tricks, the manipulation of behaviour often through deception, to gain required information. Impersonation, email, and phising are common methods used in social engineering.
- ***Illicit Collusion*** – a tactic where the cybercrime is committed by willing parties. Parties involved in the cybercrime may be internal, external, or both and may also be known, unknown or both.

4.2.5 Impact

An impact is a direct consequence of the attacker's action(s). For example, business/service disruption, data loss, data corruption, equipment damage, increased access and theft of resources.

4.2.6 Result

A result is a direct consequence of the impact. For example, financial loss, reputational damage and/or no harm done.

4.2.7 Relationship
Relationship identifies the way in which the attacker is related to the victim of the cybercrime. Internal, external, known and unknown are examples of relationships.

4.2.8 Target
A target is an object at which a cybercrime is aimed. An object could be an individual or private household, group, organization, government, country, a system or infrastructure (local or global), as well as combinations of these.

4.2.9 Offence
Offence is the legal label for the crime in the specified jurisdiction. Examples of offences that constitute crimes within the meaning of the Jamaica Cybercrimes Act are unauthorized access to program or data on a computer or on computer systems, interception of electronic transactions communications, such as website defacement, and denial of service attacks.

5. Conclusions
Although several taxonomies for cybercrimes are proposed, to date, no single taxonomy has emerged that majority crime stakeholders use. When trying to apply these schemes to our data, we found that these taxonomies were inadequate. Therefore, we developed a more comprehensive taxonomy for the organization, classification and analysis of our data. This is an essential step towards getting a better understanding of the phenomenon of cybercrime in Jamaica. In fact Moitra (2004) states that in order to develop appropriate models of cybercrime processes and patterns, it is first necessary to develop an appropriate taxonomy. Wall (2001) supports this view by stating that it is important to disaggregate cybercrimes by types as they each invoke different policy responses. Thus, an appropriate and comprehensive taxonomy is essential to developing effective investigative strategies and policies. The proposed taxonomy is an initial attempt at such a taxonomy.

Before developing our taxonomy, we identify properties that a good taxonomy should consist of. Of note, our taxonomy satisfies all properties except complete, usefulness and accepted; three properties that can only be satisfied over time, through successful classifications of actual cybercrimes, when the taxonomy is applied to data. Our proposed taxonomy is quite general, in that any particular instance of a cybercrime, known or new, can be easily classified using the scheme. This is as a result of the characteristic structure design approach used in developing the taxonomy. This design approach has been successfully used for developing taxonomies for classifying computer and network attacks. We propose that any cybercrime can be classified using these characteristics: Victim, Attacker, Objective, Tool & Tactic, Impact, Result, Relationship, Target and Offence. By centering the taxonomy on these characteristics, the taxonomy can easily and tidily classify blended cybercrimes, a limitation of previously proposed taxonomies. An advantage of this type of taxonomy is that it is not easily outdated, an important feature for a cybercrime taxonomy, given rapidly changing technologies, which create exponential opportunities for new cybercrimes.

We have created the cybercrime taxonomy *a priori*, however, we intend to use actual cybercrime data already collected to validate as well as to revise the taxonomy as necessary. This approach is consistent with the paradigm of inquiry suggested by Tukey (1980), that much can be learned by employing both *a priori* conceptualization/deduction and *a posteriori* empiricism/induction. Our proposed taxonomy aims to be a practical, specific taxonomy that can be used by information bodies to classify new cybercrimes.

References

Alkaabi, A., Mohay, G. M., McCullagh, A. J., & Chantler, A. N. (2010, October 4-6,). *Dealing with the Problem of Cybercrime.* Paper presented at the 2nd International ICST Conference on Digital Forensics & Cyber Crime, Abu Dhabi, United Arab Emirates.

Amoroso, E. G. (1994). *Fundamentals of Computer Security Technology*. Upper Saddle, NJ: Printice-Hall.

Associated Press. (2012). Jamaican Lottery Scams Spread Despite US Crackdown. Retrieved from http://www.foxnews.com/world/2012/04/17/jamaican-lottery-scams-spread-despite-us-crackdown

Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara, California: Praeger.

Canadian Centre for Justice Statistics. (2002). Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics. Retrieved from http://publications.gc.ca/Collection/Statcan/85-558-X/85-558-XIE2002001.pdf

Carter, D. L. (1995). Computer Crime Categories: How Techno-Criminals Operate. *FBI Law Enforcement Bulletin, 64*(7), 21-27.

Choo, K.-K. R., Smith, R. G., & McCusker, R. (2007). Future Directions inTechnology-enabled Crime: 2007–09 *Research and Public Policy Series* (pp. 1-166). Australia: Australian Institute of Criminology.

Chopitea, T. (2012). *Threat Modelling of Hacktivist Groups: Organization, Chain of Command, and Attack Methods.* (MSc), Chalmers University of Technology and University of Gothenburg, Göteborg, Sweden.

Clinard, M. B., Quinney, R., & Wildeman, J. (1994). *Criminal Behavior Systems: A Typology* (3rd ed.). Cincinnati, OH: Anderson Publishing Company.

Cohen, F. B. (1997). Information System Attacks: A Preliminary Classification Scheme. *Computers & Security, 16*(1), 29-46.

Furnell, S. M. (2001). *The Problem of Categorising Cybercrime and Cybercriminals.* Paper presented at the 2nd Australian Information Warfare and Security Conference, Perth, Australia.

Glass, R. L., & Vessey, I. (1995). Contemporary Application-Domain Taxonomies. *IEEE Software, 12*(4), 63-76.

Gordon, S., & Ford, R. (2006). On the Definition and Classification of Cybercrime. *Journal in Computer Virology, 2*(1), 13-20.

HaId, S. L. N., & Pedersen, J. M. (2012, February 19-22). *An Updated Taxonomy for Characterizing Hackers According to Their Threat Properties.* Paper presented at the 2012 14th International Conference on Advanced Communication Technology (ICACT 2012), Pyeongchang, South Korea.

Hansman, S., & Hunt, R. (2005). A Taxonomy of Network and Computer Attacks. *Computers & Security, 24*(1), 31-43.

Henry, P. (2009, August 30). Cyber-Related Crimes on the Increase, say Police, *Jamaica Observer*. Retrieved from http://www.jamaicaobserver.com/news/158518_cyber-related-crimes-on-the-increase--say-police#ixzz22DyDzY8E

Howard, J. D. (1997). *An Analysis of Security Incidents On The Internet 1989 - 1995.* (Doctor of Philosophy), Carnegie Melon, Pittsburg, Pennslyvania. Retrieved from http://www.cert.org/archive/pdf/JHThesis.pdf

Howard, J. D., & Longstaff, T. A. (1998). A Common Language for Computer Security Incidents: Sandia National Laboratories.

Hunton, P. (2009). The Growing Phenomenon of Crime and the Internet: A Cybercrime Execution and Analysis Model. *Computer Law & Security Review, 25*, 528–535.

Kowalksi, E., Cappelli, D., & Moore, A. (2008). Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector. Pittsburgh, PA: Carnegie Mellon Software Engineering Institute.

Krsul, I. V. (1998). *Software Vulnerability Analysis.* (Doctor of Philosophy), Purdue University. Retrieved from www.krsul.org/ivan/articles/main.pdf

Land, L., Smith, S., & Pang, V. (2013). *Building a Taxonomy for Cybercrimes.* Paper presented at the Pacific Asia Conference on Information Systems (PACIS). Paper 109.

Lindqvist, U., & Jonsson, E. (1997). *How to Systematically Classify Computer Security Intrusions.* Paper presented at the IEEE Symposium on Security and Privacy, Oakland, CA.

Lough, D. L. (2001). *A Taxonomy of Computers with Applications to Wireless Networks.* (Doctor of Philisophy), Virginia Polytechnic Institute and State University, Blacksburg, Virginia. Retrieved from http://scholar.lib.vt.edu/theses/available/etd-04252001-234145/unrestricted/lough.dissertation.pdf

Meyers, C., Powers, S., & Faissol, D. (2009). Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches: Lawrence Livermore National Laboratory.

Moitra, S. D. (2004). Cybercrime: Towards an Assessment of its Nature and Impact. *International Journal of Comparative and Applied Criminal Justice, 28*(2), 105-123.

Pfleeger, C. P. (1997). *Security in Computing* (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2004). Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector. Pittsburgh, PA: Carnegie Mellon Software Engineering Institute.

Reynolds-Baker, A. (2012). Jamaicans Warned About Putting Personal Information on the Internet Retrieved September 11, 2012, from www.jis.gov.jm/news/list/31660

Rogers, M. K. (2006). A Two-dimensional Circumplex approach to the Development of a Hacker Taxonomy. *Digital Investigation, 3*(2), 97-102.

Russell, D., & Gangemi, G. T. (1991). *Computer Security Basics*. Sebastopol, CA: O'Riley Media.

Shinder, D. L. (2003). *Scene of the Cybercrime: Computer Forensics Handbook*: Syngress Publishing.

Smith, R. G., Grabosky, P. N., & Urbas, G. F. (2004). *Cyber Criminals on Trial*. Cambridge, UK: Cambridge University Press.

Title, C. R., & Paternoster, R. (2000). *Social Deviance and Crime: An Organizational and Theoretical Approach* Roxbury Publishing Company.

Tukey, J. W. (1980). We Need Both Exploratory and Confirmatory. *The American Statistician 34*(1), 23-25.
Undercoffer, J., Pinkston, J., Joshi, A., & Finin, T. (2003). *A Target-Centric Ontology for Intrusion Detection.* Paper presented at the International Joint Conference on Artificial Intelligence, Acapulco, Mexico.
Urbas, G., & Choo, K.-K. R. (2008). Resource Materials on Technology-Enabled Crime *Technical and Background Paper*: Australian Institute of Criminology (Canberra).
Walden, I. (2007). From Computer Abuse to Cybercrime *Computer Crimes and Digital Investigations* (pp. 11-201). Oxford, UK: Oxford University Press.
Wall, D. S. (Ed.). (2001). *Crime and the Internet*: Routledge.