University of South Florida

DIGITAL COMMONS
@ UNIVERSITY OF SOUTH FLORIDA

Digital Commons @ University of South Florida

Criminology Sarasota Manatee Campus Faculty Publications

Criminology

6-2017

Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime

Fawn T. Ngo
University of South Florida, fawnngo@usf.edu

K. Jaishankar
Raksha Shakti University

Follow this and additional works at: https://digitalcommons.usf.edu/cjp_facpub_sm

Scholar Commons Citation

Ngo, Fawn T. and Jaishankar, K., "Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime" (2017). *Criminology Sarasota Manatee Campus Faculty Publications*. 4.
https://digitalcommons.usf.edu/cjp_facpub_sm/4

This Article is brought to you for free and open access by the Criminology at Digital Commons @ University of South Florida. It has been accepted for inclusion in Criminology Sarasota Manatee Campus Faculty Publications by an authorized administrator of Digital Commons @ University of South Florida. For more information, please contact digitalcommons@usf.edu.

Copyright © 2017 International Journal of Cyber Criminology – ISSN: 0973-5089
January – June 2017. Vol. 11(1): 1–9. DOI: 10.5281/zenodo.495762
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

This is a Diamond Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

SPECIAL ARTICLE

Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime

Fawn Ngo[1]
University of South Florida Sarasota-Manatee, United States of America

K. Jaishankar[2]
Raksha Shakti University, Ahmedabad, India

Abstract

The International Journal of Cyber Criminology (IJCC) is an interdisciplinary journal published biannually and devoted to the study of cyber crime, cyber criminal behavior, cyber victims, cyber laws and cyber policy. Ten years back in 2007, IJCC was launched by its founder Publisher and Editor-in-Chief K. Jaishankar with its website www.cybercrimejournal.com and with its launch, a new sub-academic discipline of Criminology, Cyber Criminology is born. IJCC is an unique Diamond open access international journal, where the authors or the readers need not pay and open to all and it is freely accessible. IJCC is indexed in prestigious databases such as Scopus & Directory of Open Access Journals (DOAJ) and IJCC's Hirsch's h-index Journal impact is 23. The International Journal of Cyber Criminology (IJCC) is commemorating its decade in existence in 2017 and we felt it would be pertinent to bring out a special article with a Research Agenda. In this article, we outline five areas that need to be addressed for the advancement of Cyber Criminology and scholarship on cyber crime and we hope this will be positively addressed by the contemporary and future Cyber Criminologists.

Keywords: IJCC, Cyber Criminology, Decade, Research Agenda, Cyber Crime.

[1] Associate Editor, International Journal of Cyber Criminology (www.cybercrimejournal.com); Associate Professor of Criminology, College of Liberal Arts & Social Sciences, University of South Florida Sarasota-Manatee, 8350 N. Tamiami Trail, Sarasota FL 34243, United States of America. Email: fawnngo@sar.usf.edu

[2] Founder – Cyber Criminology; Founding Publisher and Editor-in-Chief, International Journal of Cyber Criminology (www.cybercrimejournal.com); Professor and Head, Department of Criminology, Raksha Shakti University, Ahmedabad, Gujarat, India. E-mail: ijcc@cybercrimejournal.com

© 2017 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Introduction

In 2013, approximately 40% of the world population had access to the Internet. There is evidence that the rate of adoption of the Internet doubles every 100 days (Department of Commerce, 1998). A recent search of prior literature also reveals over 30 different types of offenses that fall under the umbrella of cyber crime including hacking, malware, identity theft, online fraud, credit card fraud, spamming, web and email spoofing, dating scam, cyber bullying, harassment and stalking, and distributed denial of service attacks. Accordingly, as the number of people worldwide using the Internet to socialize, access information, and conduct business increases, cyber crime presents significant and increasing threats to Internet users, consumers, businesses, financial institutions, and governments all over the world. Additionally, as a global criminal phenomenon, cyber crime presents issues and challenges for law enforcement officials and prosecutors who are tasked with investigating, apprehending, and prosecuting cyber criminals.

The financial consequences of cyber crime are also substantial and dire. According to a report by Symantec Corporation, a security software manufacturer, cyber crime is costing the global market an estimate of $110 billion each year. Still, another security software manufacturer, McAfee Incorporated, claims that the true annual cost worldwide from cyber crime is much higher, at around $1 trillion (Hyman, 2013). Although the precise magnitude of the financial cost of cyber crime remains unknown, what is known is that cyber crime is increasing at an increasingly rapid pace (Winmill, Metcalf & Band, 2000).

Interests in cyber crime over the last two decades have culminated in a sizable and growing body of literature. However, there are research gaps in the extant body of knowledge. For instance, there is a lack of reliable and valid statistics on the prevalence, nature, and trends of cyber crime. There is also a dearth of research on the best practices related to combating and preventing cyber crime. In this article, we outline and propose five salient and pertinent areas of inquiry relating to cyber crime for researchers, scholars, and practitioners interested in understanding, combating, and preventing this type of crime. Although our list of suggested topics is by no means represents a comprehensive research agenda, we feel these five areas of inquiry constitute a sufficient basis to advance our knowledge and the scholarship on cyber crime.

Area 1: Defining and Classifying Cybercrime

Currently, a universally agreed-upon definition of cyber crime does not exist. Further, various terminologies are being used interchangeably with the term *cyber crime,* including *computer crime*, *Internet crime, computer-related crime, online crime, high tech crime, electronic crime, technology crime,* and *information age crime*. To be sure, attempts to define and classify cyber crime have been undertaking by researchers, private businesses, government agencies, and intergovernmental organizations. For instance, the U.S. Department of Justice defines cyber crime as any crime that uses or targets computer networks. The United Kingdom Association of Chief Police Officers classifies cyber crime as any crime facilitated or committed using networked computers, telecommunications, or Internet technology. The Council of Europe's Convention on Cybercrime delineates cyber crime as offenses ranging from criminal activity against data to content to copyright infringement. Arguably, the most widely adopted definition of cyber crime is: any crime committed using computers, computer networks, or hardware devices (Gordon & Ford, 2006). Also,

© 2017 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Halder and Jaishankar (2011) have provided a definition of cyber crime from a holistic perspective:

> Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS).

Several taxonomies have also been proposed to classify the varied types of cyber crime. Wall (2001, pp. 3-7) has divided cyber crime into four categories:

> 1. Cyber-trespass – crossing boundaries into other people's property and/or causing damage, e.g. hacking, defacement, viruses. 2. Cyber-deceptions and thefts – stealing (money, property), such as credit card fraud or intellectual property violations (a.k.a. piracy). 3. Cyber-pornography. 4. Cyber-violence – doing psychological harm to, or inciting physical harm against others, thereby breaching laws pertaining to the protection of the person, such as hate speech or stalking.

Further, Wall (2005, revised in 2010, p. 82) presented cyber crime from four angles:

> 1. Crime against machines especially integrity related crimes encourage opportunities like harmful trespass. 2. Crimes using machines like computer related crimes may encourage crimes such as acquisition of domain or profile like theft or deception. 3. Crimes in the machine, such as content related crimes may encourage obscenity which may further form traditional crimes like trading sexual materials; hybrid crimes like online sex trade, Cam-girl sites and also true cyber crimes like cyber sex and cyber pimping and 4. Crimes in the machine, especially content related crimes may also encourage violence which may further motivate traditional crimes like stalking and personal harassment.

Alkaabi and colleagues (2010) proposed a classification model of cyber crime based on the role of the computer, the detailed nature of the crime, and the context surrounding the crime. The proposed model includes two types of classification, Type I and Type II offenses. Type I offenses encompass illicit activities where the computer, computer network, or electronic device is the *target* of the criminal activity and Type II offenses include illicit activities where the computer, computer network, or electronic device is the *tool* for the crime. The authors further categorized Type I offenses into four sub-groups: 1) unauthorized access offenses such as hacking; 2) malicious code offenses such as computer viruses or worms; 3) interruption of services offenses such as distributed denial of service attacks; and 4) theft or misuse of services offenses such as identity theft. Type II offenses consist of three sub-categories: 1) content violation offenses such as possessing child pornography; 2) unauthorized alteration of data or software for personal or organizational gain offenses such as online fraud; and 3) improper use of telecommunications offenses such as cyber stalking.

Defining and classifying the different types of cyber crime is a salient and pertinent area of inquiry for a number of reasons. First, having an agreed-upon definition provides

© 2017 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

scholars, researchers, and practitioners with a common language to facilitate effective collaboration and meaningful discussion. Second, having a clear definition of what cyber crime entails helps researchers and practitioners determine the scope of the problem to be addressed. Third, understanding the different aspects of cyber crime (e.g., differentiating the "technical" versus "people" dimensions of cyber crime) could assist law enforcement and criminal justice agencies investigate, combat, and prevent this type of crime. Finally, defining and differentiating the different types of cyber crime enables researchers and practitioners to predict the direction of future cyber crime as well as formulate novel and timely solutions.

Area 2: Assessing the Prevalence, Nature, and Trends of Cybercrime

Currently, there is a lack of reliable and valid statistics on the prevalence, nature, trends, and impact - particularly financial impact - of cyber crime. Obtaining reliable and valid statistics on cyber crime is a salient and pertinent area of inquiry because such data are germane for enhancing local and national responses to cyber crime, educating the public about this type of crime, implementing effective prevention strategies, providing intelligence and risk assessment, facilitating crime reporting, and identifying areas for research. It is noteworthy that law enforcement agencies and private industries do collect data on cyber crime but official data such as police data are often under-reported or under-recorded for a variety of reasons such as victims not realizing that they have been victimized or victims assuming that police responses will be ineffective (Halder & Jaishankar, 2016; Jaishankar, 2015). Under-reporting could also stem from a fear of negative publicity or a lack of incentive (Halder & Jaishankar, 2015; Jaishankar & Halder, Forthcoming). Likewise, data provided by private industries should be viewed with caution particularly when these companies have a vested interest in promoting their products or services. Accordingly, attaining reliable and valid statistics on cyber crime warrants the collection of both official and self-report data as well as the implementation of appropriate research designs and methodologies.

Area 3: Advancing the Field of Cyber Criminology

Cyber Criminology is a sub-academic discipline of Criminology founded by K. Jaishankar in 2007 and he academically coined the term "cyber criminology" and launched the first ever journal dedicated to the advancement of the field of Cyber Criminology and scholarship on cyber crime, i.e., International Journal of Cyber Criminology (www.cybercrimejournal.com). Cyber Criminology denotes "the study of causation of crimes that occur in the cyberspace and its impact in the physical space" (Jaishankar, 2007, p.1). As an academic discipline, cyber criminology encompasses multidisciplinary field of inquiry including criminology, sociology, victimology, and computer sciences. At its core, cyber criminology involves the examination of criminal behavior and victimization in cyber space from a criminological or behavioral theoretical perspective (Jaishankar, 2010, 2011). Stalans and Finn (2016, pp. 502-503) mentions: "The field is young, but has begun to amass scholarship on many forms of cyber crime, including book collections featuring research throughout the globe (e.g., Jaishankar, 2011; Kshetri, 2013; Wall, 2007) and *six* (*emphasis ours*) reviews on the current state of knowledge" (Choi, 2015; Diamond & Bachmann, 2015; Holt & Bossler, 2014; Nhan & Bachmann, 2010; Stalans & Finn, 2016; França, Forthcoming, 2018).

© 2017 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Though, Nhan and Bachmann (2010), feels that "Cyber criminology is slowly emerging from a niche area that is often marginalized by mainstream criminology to one of high importance" (p. 175) it is still neglected and marginalized by mainstream criminology (Diamond & Bachmann, 2015). This fact is unfortunate given the current number of Internet users worldwide and the real and serious threats that cyber crime poses for these individuals. Advancing the field of cyber criminology is a salient and pertinent area of inquiry (Jaishankar, 2010) because unlike traditional crime or crime committed in the physical world, cyber crime or crime committed in the virtual world has the potential of causing tremendous damage, both tangible (i.e., economic loss) and intangible (e.g., the unauthorized use of personal data). Specifically, whereas traditional crime tends to be one-to-one crime or a crime that starts when the victimization of the target is begun and ends when the victimization of the target is concluded, cyber crime is considered to be one-to-many crime in that cyber crime can be automated with the perpetrator employing technology to execute many criminal activities within a given period of time (Brenner, 2004). Further, compared to traditional crime, it is much more difficult to identify and apprehend cyber criminals because they can use technology to conceal their identities and physical locations (Wall, 2011).

To date, etiological and victimization research on cyber crime generally involve mainstream criminological perspectives, namely, routine activities theory (Cohen & Felson, 1979), self-control theory (Gottfredson & Hirschi, 1990), social learning theory (Akers, 1998), and techniques of neutralization (Sykes & Matza, 1957). The debate on the efficacy of existing criminological perspectives, which were developed to account for crime committed in the physical world, to account for crime committed in the virtual world has led to the development of new theoretical frameworks, such as space transition theory (Jaishankar, 2007, 2008) which is credited by many scholars as a noteworthy contribution to the field of criminology in general and cyber criminology in particular (Diamond & Bachmann, 2015; Holt & Bossler, 2014, 2016; Holt, Bossler, Spellar, 2015; Moore, 2012, Wada, Longe, & Danquah, 2012). While there is evidence that mainstream theories can be successfully apply to various forms of cyber crime (see for example, Holt, Bossler & May, 2011; Morris, 2011; Ngo & Paternoster, 2011; Pratt, Holtfreter & Reisig, 2010), there is a dearth of research examining the applicability and efficacy of novel theoretical perspectives such as space transition theory *(Notably, space transition theory was empirically tested by Zhang (2009) (cyber bullying) and Danqua and Longe (2011).* To advance the field of cyber criminology and our knowledge and understanding of criminal behavior and victimization in cyber space, research examining which theoretical framework best account for which substantive type of cyber crime employing both traditional and new perspectives should be undertaken.

Area 4: Documenting Best Practices in Combating and Preventing Cybercrime

The evidence-based movement that permeated the field of criminal justice and criminology in the 1990s calls for the inclusion of high-quality scientific evidence in the formulation and implementation of criminal justice intervention and prevention strategies. To aid policy makers, practitioners, and the public make informed decisions regarding crime and justice policies, the Campbell Collaboration was inaugurated in 2000 in Philadelphia with 100 representatives from 15 countries in attendance. The Campbell Collaboration is an international volunteer network of policy makers, researchers, practitioners, and consumers who prepare, maintain, and disseminate systematic reviews of

© 2017 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

research studies on intervention programs in the social and behavioral sciences (see http//:www.campbellcollaboration.org). The Campbell Collaboration was modeled after the international Cochrane Collaboration that prepare, maintain, and disseminate systematic reviews on what works, what doesn't, and what is promising in the arena of medicine and health care (see http//:www.cochranecollaboration.org).

Currently there exist only a handful of systematic reviews on the subject of cyber crime and to the best of our knowledge; no study has examined what works and what doesn't work in combating and preventing cyber crime. Documenting best practices in combating and preventing cyber crime is a salient and pertinent area of inquiry because there is evidence that conventional policing methods designed to fight and prevent crime in the physical space are ill suited for combating and preventing crime in the virtual world (Jones, 2007). Notably, given that cyber crime is a global phenomenon and the tools of cyber criminals are technology and anonymity, research examining the effectiveness of collaborative efforts between law enforcement and private entities (e.g., security software manufacturers, software development companies) and between cross-national law enforcement agencies are warranted. Relatedly, since the investigation and prosecution of cyber crime involve digital evidence (i.e., evidence in the form of data extracted from a computer), research studies evaluating the usefulness of computer forensic techniques in retrieving and preserving digital data are also warranted.

Area 5: Cybercrime and Privacy Issues

The protection of citizen privacy in the investigation and prosecution of cyber crime is perhaps one of the most controversial and hotly debated topics in recent years. As an example, the introduction and growth of information and communication technologies (ICTs) have enabled individuals to use email and mobile devices to communicate with friends, family, and business associates across the globe. However, in the course of sending an email, the Internet users may produce an array of information that is potentially relevant to or subjected to a criminal offense investigation. Should such information remain private? Similarly, nowadays commercial organizations – particularly Internet service and social networking platform providers – collect and sell personal data which either the clients consent to or which were collected without the client's knowledge. Further, these commercial organizations can themselves become victims of cyber crime such as online theft of data or the infection and spread of malware. Should there be privacy safeguards against the commercialization and exploitation of personal data? Additionally, because all digital activities leave traces that can be linked to personal data, this could potentially lead to the surveillance of Internet users (e.g., Muslim Americans) by all kinds of operators (e.g., the U.S. Department of Homeland Security).

Hence, examining and exploring ways to ensure the protection of citizen privacy in the investigation and prosecution of cyber crime is a salient and pertinent area of inquiry since the right to privacy is protected under many national constitutions and is also an element of various legal traditions. In addition to searching for a balance between public safety and personal autonomy, the issue regarding anonymity in cyber space should also be explored. Anonymity in cyberspace is a significant topic - and concern - for the global community because it is considered the cornerstone of democracy as well as related to the notion of "freedom of expression." Anonymity allows individuals to express their views online without fear of reprisals and public hostility. In some parts of the world, anonymity also

© 2017 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

permits individuals to express their opinions without being linked to certain published views. However, anonymity in cyber space also provides criminals with the means of perpetrating harms to the masses with little chance of apprehension. Accordingly, determining whether anonymity in cyber space should be permitted or not as well as to what extent limitations on anonymity in cyber space should required will make valuable contributions to the scholarship on cyber crime.

Conclusion

The growing threat of cyber crime is real and serious. The new breed of criminal activities and offenders in cyber space also present law enforcement officials and prosecutors with issues and challenges in the investigating of cyber crime and prosecuting of cyber criminals. While there exists a sizable and growing body of literature on cyber crime, there are also research gaps that need to be addressed. In this article, we outline and propose five salient and pertinent areas of inquiry that we feel constitutes a sufficient basis to advance our knowledge and the scholarship on cyber crime. We hope our proposed agenda will serve as a helpful guide for researchers, scholars, and practitioners interested in understanding, combating, and preventing cyber crime.

References

Akers, R. L. (1998). *Social Learning and Social Structure: A General Theory of Crime and Deviance*. Boston: Northeastern University Press.

Alkaabi, A., Mohay, G., Mucullagh, A., & Chantler, N. (2010). Dealing with the problem of cyber crime. In: Baggili I. (eds.), *Digital Forensics and Cyber Crime* (1-18). Berlin, Heidelberg: Springer.

Bossler, A. M., Holt, T. J., & May, D. (2011). Predicting Online Harassment Victimization Among a Juvenile Population. *Youth & Society, 4*, 500-523.

Brenner, S. W. (2004). Cybercrime metrics: *Old wine, new bottles? Virginia Journal of Law and Technology*, 9, 1-53.

Cohen, L. E., & Felson, M. (1978). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*, 588-608.

Choi, K. S. (2015). *Cybercriminology and Digital Investigation*. El Paso, Texas: LFB Scholarly Publishing LLC.

Danquah, P., & Longe, O. (2011). An empirical test of the space transition theory of cyber criminality: Investigating cyber crime causation factors in Ghana. *African Journal of Computing & ICT*, *2*(1), 37-48.

Department of Commerce (1998). *The emerging digital Economy* [On-line]. Retrieved from https://www.esa.doc.gov/sites/default/files/emergingdig_0.pdf.

Diamond, A., & Bachmann, M. (2015). Out of the beta phase: Obstacles, challenges, and promising paths in the study of cyber criminology. *International Journal of Cyber Criminology, 9*, 24-34.

França, L. A. (Forthcoming 2018). Cyber-Criminologies. In P. Carlen and L. A. França, (Eds.), *Alternative Criminologies*. Abington, Oxford, UK: Routledge.

Gordon, S., & Ford, R. (2006). On the definition and classification of cyber crime. *Journal of Computer Virology, 2*, 13-20.

Gottfredson, M. R., & Hirschi, T. (1990). *A General Theory of Crime*. Stanford, CA: Stanford University Press.

© 2017 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Halder, D., & Jaishankar, K. (2015). Irrational Coping Theory and Positive Criminology: A Frame Work to Protect Victims of Cyber Crime. In N. Ronel and D. Segev (eds.), *Positive Criminology* (pp.276 -291). Abingdon, Oxon: Routledge. ISBN 978-0-415-74856-8.

Halder, D., & Jaishankar, K. (2016). Policing Initiatives and Limitations. In: J. Navarro, S. Clevenger, and C. D. Marcum (eds.), *The Intersection between Intimate Partner Abuse, Technology, and Cyber crime: Examining the Virtual Enemy* (pp. 167-186). Durham, North Carolina: Carolina Academic Press.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cyber crime scholarship. *Deviant Behavior, 35,* 20–40. doi:10.1080/01639625.2013.822209

Holt, T., Bossler, A. M., & Spellar, S. K. (2015). *Cyber crime and Digital Forensics*. Abingdon, Oxon: Routledge.

Holt, T., & Bossler, A. M. (2016). *Cyber crime in Progress: Theory and Prevention of Technology-enabled Offenses*. Abingdon, Oxon: Routledge.

Hyman, P. (2013). Cybercrime: It's serious, but exactly how serious? *Communications of the ACM*, 56, 18–20.

Jaishankar, K. (2007). Establishing a theory of cyber crimes. *International Journal of Cyber Criminology, 1*, 7-9.

Jaishankar K., (2008). Space transition theory of cyber crimes. In F. Schmallager and M. Pittaro (Eds.), *Crimes of the Internet* (pp.283-301). Upper Saddle River, NJ: Prentice Hall.

Jaishankar, K. (2010). The Future of Cyber Criminology: Challenges and Opportunities. *International Journal of Cyber Criminology*, *4*(1&2), 26–31.

Jaishankar, K. (2011). Introduction / Conclusion. In K. Jaishankar (Ed.), *Cyber criminology: Exploring Internet crimes and criminal behavior* (pp. xxvii–xxxv and pp. 411-414). Boca Raton, FL: CRC Press.

Jaishankar, K. (2015). *"Cyber crime Victimization: New Wine into Old Wineskins?"*, Keynote Speech at the 15th World Society of Victimology Symposium, July 5-9, 2015, at Perth, Australia, organized by Victim Support, Angelhands Inc. and supported by Australian Institute of Criminology.

Jaishankar, K. & Halder, D. (Forthcoming). *Cyber Victimology: Decoding Cyber Crime Victimization*. Boca Raton, FL, USA: CRC Press, Taylor and Francis Group. ISBN: 978-14-987848-9-4.

Jones, B. R. (2007). Virtual neighborhood watch: Open source software and community policing against cyber crime. *Journal of Criminal Law and Criminology, 9*7, 601-630.

Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south*. New York, NY: Palgrave MacMillan Publishers.

Moore, R. (2012). *Cyber crime: Investigating High-Technology Computer Crime*. Abingdon, Oxon: Routledge.

Morris, R. G. (2011). Computer hacking and the techniques of neutralization: An empirical assessment. In T. J. Holt and B. H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and Implications* (pp. 1-17). IGI Global: Hershey, PA.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*, 773-793.

© 2017 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License

Nhan, J., & Bachmann, M. (2010). Developments in cyber criminology. In M. Maguire & D. Okada (Eds.), *Critical issues in crime and justice: Thought, policy, and practice* (pp. 164–183). Thousand Oaks, CA: Sage.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*, 267-296.

Stalans L. J. & Finn, M. A., (2016). Understanding How the Internet Facilitates Crime and Deviance. Victims & Offenders, *11*(4), 501-508.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*, 664-670.

Wada, F., Longe, & O. Danquah (2012). Action Speaks Louder than Words-Understanding Cyber Criminal Behavior Using Criminological Theories. *Journal of Internet Banking and Commerce, 17*(1), 1.

Wall, D. S. (2005, revised in 2010). The internet as a conduit for criminal activity. In A. Pattavina (Ed.), *Information technology and the criminal justice system* (pp. 78-94). Thousand Oaks, CA: Sage Publications.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age.* Malden, MA: Polity Press.

Wall, D. S. (2001). Cyber crimes and the internet. In D. Wall (ed.) *Crime and the internet* (pp. 1-17). London: Routledge.

Wall, D. S. (2011). Policing Cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research: An International Journal,* 8, 183-205.

Windmill, L. B., Metcalf, D. L., & Band, M. E. (2000). Cybercrime: Issues and challenges in the United States. *Digital Evidence and Electronic Signature Law Review,* 7, 19-34.

Zhang, X. H. (2009). An Exploration of Student Teachers' Interaction with on-line activities, and their influence on their teaching topics such as netiquette and cyber-bullying: An Australian and Chinese Study. Doctoral Thesis submitted to the Griffith University, Australia. Retrieved from https://www120.secure.griffith.edu.au/rch/file/cf7a4f3e-5132-1570-f88e-8efd334cf8d1/1/Zhang_2001_02Thesis.pdf

© 2017 International Journal of Cyber Criminology (Diamond Open Access Journal). Under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License