ISSN: 0973-5089 - January – June 2015. Vol. 9 (1): 24–34. DOI: 10.5281/zenodo.22196

Out of the Beta Phase: Obstacles, Challenges, and Promising Paths in the Study of Cyber Criminology[1]

Brie Diamond[2] & Michael Bachmann[3]
Texas Christian University, United States of America

Abstract

The article provides an overview of the current state of cyber criminological study with regard to theory, research, and teaching. In contrast to the vast knowledge about technical aspects of cyber crimes, behavioral research on these offenses is currently still in its infancy with few data sources or publication outlets. This article will detail the fundamental issues and problems facing researchers involved in the young discipline of cyber criminology, ranging from definitional to methodological problems. There remains argument amongst cyber crime scholars over how best to define the focus of the field and numerous theoretical explanations compete for preference with the scholarly community. These issues pose significant obstacles and need to be addressed for the discipline to advance. Suggestions of how to address some of the primary issues are provided and potential solutions are presented.

Keywords: Cyber Criminology, Definitional and Methodological Problems, Research problems, Discipline Development.

Introduction

Computers have become an integral part of every aspect of our lives. Computer technologies are relied on for nearly everything we do and we live in societies that are fundamentally dependent on digital infrastructure for their continued functioning. Increasingly, this mission-critical nature of computer networks for nearly all industry sectors, combined with the wealth of personal information that is being put online, has bred a new type of dangerous criminal—one that is targeting computers to steal our information, finances, and personal identifications (Bachmann & Corzine, 2009; Furnell, 2002; Holt, 2010; Jaishankar, 2007, 2008; Jewkes, 2007; Nhan & Bachmann, 2010; Yar, 2006). The Office of the President of the United States suggests that threat posed by these

[1] Revised version of the Keynote Lecture delivered by the corresponding author at the Second International Conference of the South Asian Society of Criminology and Victimology (SASCV) at Kanyakumari, Tamil Nadu, India, held during 11-13, January 2013.

[2] Assistant Professor of Criminal Justice, Texas Christian University, TCU BOX 298720, Fort Worth, TX 76129, USA. Email: b.diamond@tcu.edu.

[3] Associate Professor of Criminal Justice, Texas Christian University, TCU BOX 298720, Fort Worth, TX 76129, USA. Email: m.bachmann@tcu.edu (Corresponding Author).

cyber-criminals "is one of the most serious economic and national security challenges" (2009, para, 18).

Today, governments around the globe struggle to employ effective countermeasures against cyber-attacks. The implementation of such countermeasures is increasingly facilitated by the vast amount of scientific knowledge about the technical details of the various attack methods (Amoroso, 2011). Unfortunately, the guidance provided by these studies is limited to details on the methods of attack and is left lacking insight about who the attackers are and how they differ from "traditional" criminals. This situation persists despite the concerted efforts of a small number of dedicated scholars from around the globe (among them Bachmann, Brenner, Hinduja, Holt, Jaishankar, Jewkes, Kilger, Nhan, Turgeman-Goldschmidt, Patchin, Wall, Yar, to name but a few) advancing a newly developing field of criminological study, called "Cyber Criminology" (Jaishankar, 2007).

For the past eight years, the young discipline, has grown with the contribution of many experts, including the exceptional efforts of its founder K. Jaishankar, who defined Cyber Criminology, as *"the study of causation of crimes that occur in the cyberspace and its impact in the physical space"* (Jaishankar, 2007; p.1). This definition accounts for the multidisciplinary nature of the field that relies upon insights from both the social (criminology and sociology) and computer sciences. Also, Jaishankar (2008) has introduced the first theory (Space Transition Theory of Cyber Crimes) exclusively developed to explain offending in cyberspace and has founded the first academic journal dedicated to the criminological study of cyber crimes, the International Journal of Cyber Criminology, http://www.cybercrimejournal.com (Jaishankar, 2007). With the contributions of international experts, this ranked journal with high quality articles and rigorous peer review has grown as a core outlet in the field of cyber criminology.

These and similar efforts aside, the fact remains that cyber criminology is largely ignored or marginalized by mainstream criminology, and that many criminologists refrain from examining this important, future-oriented issue. Whether it be that they are lacking the necessary understanding of technology, are intimidated by the jargon of the field, or that they continue to fail to realize the full extent of societal implications of this new type of crime, the lack of consideration is troubling. Others become discouraged by the multitude of methodological problems involved in conducting quantitative studies of cyber-offenders, particularly when attempting to generate representative samples of online offenders. Also, major criminological associations (e.g. the American Society for Criminology (ASC)) continue to marginalize cyber criminological studies in their annual conferences and, partly due to the many unresolved methodological problems, cyber crime researchers face significant difficulties in getting their manuscripts accepted by top tier criminological journals. Taken together, these problems systematically discourage many from studying the problems and, in turn, result in still limited, albeit rapidly increasing, numbers of annual publications.

The article addresses many of the main problems facing cyber criminologists today. It intends to shed a light on the difficulties and suggests ways to overcome them. The strengths and weaknesses of potential methods are analyzed and their implications for the interpretation and generalization of results are considered. Suggestions for future research are provided. The presentation seeks to spark a conversation with the audience about promising solutions to some of the current problems and potential approaches of how to create standards for future research in this new area of criminology.

1. Issues in defining Cyber crime

The difficulties surrounding the study of cyber crime begin at the definitional level. Should cyber crime be conceptualized as a brand new crime type or traditional crimes pursued through a new medium? Researchers such as Grabosky (2001) adhere to the former definition and regard cyber crimes to be motivated by the same basic human emotions—greed, lust and revenge—that underlie crimes committed in real space. Along the same lines, Thomas and Loader (2000, p. 3) define cyber crime as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks". However, others have argued that many cyber crimes fail to conform to the traditional model of crime. Furnell (2002) suggests a two-pronged understanding of cyber crimes—*computer-assisted* and *computer-focused* crimes. Furnell views the former, computer-assisted crimes to be "old wine in new bottles" (to use the nomenclature expressed in Grabosky, 2001) wherein crimes such as credit card fraud and cyber terrorism are committed through the use of information and communications technology (ICT), but are still capable of being conducted via traditional methods. Conversely, computer-focused crimes such as hacking and website defacement represent new crimes unparalleled in conventional crimes that necessitate the use of ICT—without which these crimes would not exist. Likewise, Smith and colleagues (Smith, Grabosky, & Urbas, 2004) draw a distinction between those crimes that use ICT in the commission of the offense versus those that are directed squarely at such technologies. Also, cyber criminologists like Wall (1999), Yar (2005) and Jaishankar (2008, 2011) ascertains that cyber crime is a new form of crime. Jaishankar (2008) explains:

> Even though some researchers feel cyber crimes as a case of "old wine in new bottles" (Grabosky, 2001), "old wine in bottles of varying and fluid shape" (Yar 2005), or "new wine in no bottles" (Wall, 1999), cyber crimes are still different from the crimes of physical space. There exists a fine line of demarcation between the crimes of physical space and crimes of cyberspace. The demarcation lies in the 'involvement of the virtual cyber medium' (Pati, 2003), 'lack of geographical boundaries' (Hafner & Markoff 1995; Mitra 1999), and 'their occurrence in a diffuse, fluid, evolving' (Brenner, 2004) and 'spatiotemporally disorganized environment' (primarily the collapse of spatial–temporal barriers, many-to-many connectivity, and the anonymity and plasticity of online identity) (Yar 2005; Williams, 2005). Yar (2005) ascertains after analyzing cyber crime with routine activities theory that cyber crime is a new and distinctive form of crime. Cyber crime is an entirely new form of crime (p. 291).

However, studies of cyber crime suffer from many of the same definitional issues common to other sub-disciplines in the field. White-collar crime, as Smith and colleagues point out, has come to include a variety of crimes that "include any acts of occupational deviance involving a breach of the law or ethical principles" (p. 10)—a definition that inhibits clarity across research endeavors. Likewise, the study of sex offending, which can entail a wide range of criminal conduct—with distinct motives and a wide range of harm to victims and society—is analogous to the difficulties surrounding cyber crime research, which can run a similar gamete of human behavior.

2. A Dearth of Data

The problems arising from the wide range of criminal behavior encapsulated by the term cyber crime is not aided by the veritable lack of data available to scrutinize these crimes. Most of the data on cyber crime come from either agency or victimization surveys. Beginning in 2004, the Census of State and Local Law Enforcement Agencies representing more than 20,00 agencies across the United States asks whether or not these agencies performed cyber crime investigations on a regular basis (United States Department of Justice, 2004). A similar survey of campus law enforcement agencies makes the same inquiries of campus agencies and shows that over half of these agencies had individuals designated to handle cyber crimes on campus (United States Department of Justice, 2004-2005). Likewise, LEMAS, the Law Enforcement Management and Administrative Statistics survey asks whether agencies handled cyber crimes via a specialized unit, designated personnel, or if they did not have any special way to handle such crimes (United States Department of Justice, 2007). While datasets such as these give a base understanding of the law enforcement resources dedicated to cyber crime, they do not provide much depth into the prevalence of or official handling of such crimes—let alone offender characteristics.

A handful of datasets provide victimization information and even fewer use offender reports of cyber crime. Since 2006 the National Crime Victimization Survey (NCVS; United States Department of Justice, 2012), a representative sample of United States households, has inquired about cyber crime victimization against members over the age of 12. Unfortunately, this single question does not disaggregate cyber crime into its various categories making the usefulness of this measure rather superficial. The Identity Theft Supplement of the NCVS collected in 2012 (United States Department of Justice), representing household members 16 years of age and older, however, does delve expressly into hacking in regard to identity theft victimization. Specifically, it asks victims of identity theft if the misuse of their personal information came to their attention due to "suspicious computer activity including email hacked". Beyond these few examples, little large-scale effort has been made to document the prevalence of cyber crime victimization.

If victimization data are rare, information on cyber crime offenders is virtually non-existent. The Survey of Inmates in State and Federal Correctional Facilities (United States Department of Justice, 2004) collects data on whether inmates used computers in the commission of a range of offenses including identity theft, obscene communication, copyright infringement, forgery and sabotage of a computer or computer system. These data, while representing an ability to delve into cyber crime offender characteristics, highlights the nascent focus on this type of crime. What exists beyond these few examples is largely small, convenient samples of college students reporting on their involvement in minor forms of cyber crime such as digital piracy (see Gunter, 2011; Higgins & Makin, 2004; Morris & Blackburn, 2009). These data represent the bulk of cyber crime research and its application of criminological theories.

3. Theoretical Issues

Flowing from the contention over the definition of cyber crime and the lack of data on the topic, theoretical advancement has been lacking. The debate over whether cyber crime is a new type of crime or old crimes committed in new ways is mirrored in the theoretical literature. Scholars disagree as to whether our current sociologically driven theories are capable of properly accounting for criminal behavior committed in the virtual

realm. While some have proposed theories such as routine activities and social learning to be adaptable to cyber crime, others have argued that a fresh theoretical approach is warranted (Jaishankar, 2008).

The problems underlying cyber criminology are two-pronged (Mar, 2005). First, many of the correlates of crime established through traditional criminology are irrelevant in regard to cyber crime. Most cyber crimes still tend to be committed by young males; however, due to the very nature of this class of crime, cyber criminals tend to be well-educated members of the middle/upper-middle class (Bachmann, 2010; Pratt, Holtfreter, & Reisig, 2010; Smith et al., 2004; Yar, 2006). The "usual suspects" of many criminological theories—minority, poorly educated offenders from the lower class—are simply priced and skilled out of computer-related crimes. Likewise, the traditional victim-offender relationship where individuals tend to know and share many common characteristics with an offender is largely irrelevant.

In a similar vein, the physical aspects of traditional crimes that have shaped criminological theory bear little to no importance in regard to cyber crimes. Flowing from the work of Shaw and McKay (1942), criminological theories have long since relied upon the confluence of offenders and victims in time and space. The rich imagery of the zone in transition—replete with characters interacting on disordered, volatile streets—sparked a wave of theories focused on the impact of the physical, social environment on human behavior. These theorists had street crimes—strong-arm robberies, residential burglaries—in mind when developing these explanations and could hardly have anticipated a genre of deviance almost completely detached from the physical environment.

Cyber crimes offer a unique opportunity for offenders to gain access to what would *sans* internet be inaccessible victims. So the question remains: can our traditional criminological theories be transposed to the virtual world? Some see our current theories being of little utility; though, attempts have been made to apply routine activity theory (RAT) to cyber crime. The problem for RAT is the heavy emphasis on the convergence of offenders and victims in physical space (see Cohen & Felson, 1979). Yar (2005) argues that the "antispatial" (quoting Mitchell, 1995) nature of cyber crime can be rectified within the existing theory.

The amorphous virtual environment may be less of an issue for the study of cyber crime than it seems. While, as Yar (2005) points out, it is impossible to predict the convergence of motivated offenders and suitable targets in the online environment, so it is largely impossible to pinpoint the convergence of these actors in real space. The internet may be "populated 24/7", but there are still times of greater traffic—introducing more offenders and targets—that may still be predictive of victimization. Regardless, most research on RAT focuses not upon the physical convergence of offenders and targets, but on the characteristics of suitable targets and their lack of guardianship. This situational foreground is the true power and focus of RAT. Likewise, applications of RAT to cyber crime should be less concerned with the fittingness of the virtual environment to the theory and focus instead on what cyber-criminals view to be a suitable target and what guardianship is deemed adequate to reduce the chances of victimization.

Yar (2005) surveys the aspects of a suitable target (proximity, exposure, attractiveness, and guardianship) outlined in RAT and concludes that these categories have mixed applicability to the virtual environment. Obviously, the idea of physical proximity is problematic for the theory, but he also dismisses the concept of exposure (visibility, as he

refers to it) as being a constant and a requirement of involvement in the online environment. Yes, visibility is inherent on the internet, but how does this differ from the inherent visibility of most individuals in the physical world? Exposure exists more along a continuum, so that the amount of exposure to motivated offenders is what matters. Likewise, the more prominent an individual's presence on the internet and across a range of websites, the greater the opportunity for their victimization, thus making them a more visible and suitable target. This position is supported by recent RAT research on online financial fraud (Pratt, Holtfreter, & Reisig, 2010). Likewise, researchers have shown that online harassment victimization depends upon the amount of time spent in chat rooms and engaged in instant messaging (Holt & Bossler, 2008). The ideas of attractiveness and capable guardianship translate nicely to suitable targets in the online environment. Those individuals or organizations that pose a financial benefit (e.g., intellectual property) or an affiliation of interest to an offender (e.g. religious, sexual or racial) will likely be deemed more attractive targets. Finally, the concept of capable guardianship translates to the virtual environment as well. Yar (2005) explains how guardianship takes on two forms: social guardianship such as the presence of network administrators or online citizens calling out cyber offenders; and physical guardianship, such as anti-virus software and firewalls.

In the end, Yar (2005) considers RAT to be of limited utility to the explanation of cyber crime. This seems largely due to the non-physical nature of the online environment and the inability to predict when and where offenders will come into contact with suitable targets. RAT, however, is a policy-focused theory that quibbles less about the environmental background that these actors move through and focuses more on the characteristics of individuals that increase their risk of victimization. As such, ignoring the role of physical proximity that is so important to crimes committed in real space, but appreciating the ways that online exposure, target attractiveness, and the absence or weakness of social and/or physical guardianship shape the victimization risk of online entities has a distinct probability of explaining crime in virtual space.

Other existing theories seem less capable of explaining cyber crime. One of the most important predictors of street-level offending, low self-control, is unlikely to be applicable to individuals who are capable of pursuing higher levels of education and employment. One would expect the findings to be quite similar to the non-significance of low self-control in predicting corporate crime (Simpson & Piquero, 2002). Holt and colleagues (Holt, Bossler & May, 2011), however, have uncovered a small, yet significant influence of low self-control on offenses committed by teenagers such as pirating media/software, hacking and viewing sexual material—a group of individuals and behaviors with a stronger link to the desire for immediate gratification than perhaps more serious forms of cyber crime (see also Higgins, 2004; Higgins & Makin, 2004). Further, the plausability of strainful life experiences being the motivation behind these crimes seems tenuous as well (although, in regard to cyberbullying see Patchin & Hinduja, 2011).

Some indications have been made, however, that social learning principles may be important in cyber offending (Holt & Bossler, 2008; Holt, Bossler, & May, 2011; Holt, Burress & Bossler, 2010; Morris, 2011; Morris & Blackburn, 2009; Morris & Higgins, 2010). Namely, association with delinquent peers appears to predict involvement in computer hacking, digital piracy and online harassment victimization. Holt, Burress and Bossler (2010) show that while differential association with cyber offenders is the most influential social learning principle, the remaining aspects of imitation, differential reinforcement and pro-delinquent definitions significantly influence cyber crime

involvement. Likewise, findings from a survey of roughly 800 college students suggests that hackers may engage in some of Sykes and Matza's (1957) techniques of neutralization, such as denial of injury or victim blaming, to justify their behavior (Morris, 2011). In conclusion, it appears that many of our existing theories can be successfully applied to various forms of cyber crime, apart from exclusive theories on cyber crime such as the space transition theory (Jaishankar, 2008). What needs to be done now is more systematic research into which theories operate best upon which categories of cyber crime and for which type of offenders.

4. Teaching Issues

Cybercrime courses are ones of particular interest to modern day students of numerous disciplines. However, programs attempting to offer such courses find themselves encountering a number of issues. Historically, college classes focused solely on cyber forensics, the practical implementation of cyber crime investigation, rather than the theoretical discipline of cyber criminology (Jaishankar, 2010). Melding the two focuses of cyber forensics and cyber criminology would lead to a more holistic educational experience for students in the field. To this end, the University of Alabama now offers a minor in cyber criminology that exposes students to the law enforcement practices, theoretical explanations, computer science ethical issues, and cyber law surrounding cyber crime (for further information, see http://courseleaf.ua.edu/artssciences/criminaljustice/#cybercrimitext). Fortunately, other undergraduate and graduate courses are already offered all over the globe and more are currently being developed. It appears that the issue of cyber crime and our understanding of its societal implications are slowly moving outside of the narrow confines of computer sciences. With more social science departments incorporating the issue into their programs, the hope remains that a next generation of social scientists will devote more attention to this pressing, vast, and growing problem. The primary challenge for such programs will be to strike an appropriate balance in incorporating technological aspects since many students in these fields are easily intimidated by the technical intricacies involved in the commission of many cyber crimes.

5. Publication Issues

Some of these theoretical endeavors have made their way into mainstream criminology journals, but most research on cyber crime is relegated to edited book volumes and more obscure journals and/or journals outside of the field altogether (Jaishankar, 2010). Further, few cyber crime-specific peer-reviewed journals exist for authors to disseminate their work to other cyber criminologists—*International Journal of Cyber Criminology* being the most prominent. The choices of outlets are expanding, however, with new journals such as the *Journal of Technology and Crime* being established. As federal interest in preventing cyber crime continues to grow, and with it the amount of data for analysis, hopefully we will see the numbers of top tier cyber crime publications grow and the prestige of these specialized journals rise. As it stands, the more creative and less conventional methodological approaches necessitated for many especially quantitative cyber crime studies renders placing these studies in top-tier journals difficult. Currently, the gradual shift on the federal level away from terrorism and toward cyber crime is already being reflected in a surge of edited and sole-authored book publications on cyber crime-related

issues. The range of topics addressed in these recent books includes classic cyber criminological studies as well as homeland and critical infrastructure protection from digital threat assessments as well as cyber-terror and cyber-warfare related issues.

Conclusion

In spite of the various issues mentioned, it should be noted, that, cyber criminology has come a long way during the short time since its conceptual inception (Jaishankar, 2007), and its developmental pace continues to accelerate. As evermore spectacular high-dollar and high-impact cyber crime heists (Douglas & Timberg, 2014), vulnerabilities, and surveillance issues (McManus, 2014) continue to grip the attention of mainstream media, society at large is becoming more aware of the severity and dangerousness of cyber crimes and related issues. The young discipline of cyber-criminology is already benefiting from this increasing awareness. More social scientists are beginning to examine cyber criminological topics and aspects, and it is safe to predict that greater numbers will follow in the years to come. Just as its subject of study, cyber criminology will become more mainstream within criminology. Hopefully, this predictable growth of the field will bring with it solutions to some of the basic problems outlined in this article that are currently still plaguing this young discipline.

References

Amoroso, E. G. (2011). *Cyber attacks: Protecting national infrastructure*. Burlington, MA: Elsevier.

Bachmann, M. (2010). Deciphering the hacker underground: First quantitative insights. In T. Holt & B. Schell (Eds.) *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 105-127). Hershey, PA: IGI Global.

Bachmann, M., & Corzine, J. (2009). Insights into the hacking underground. In T. Finnie, T. Petee & J. Jarvis (Eds.), *The future challenges of cyber crime* (Pp. 31-41). Volume 5: Proceedings of the Futures Working Group. FBI, Quantico, VA. 2010.

Brenner, S. (2004). Toward a Criminal Law for Cyberspace: Distributed Security. *Boston University Journal of Science & Technology Law*, *10*(2), 1-112.

Cohen, L. E. & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*. 44, 588-605.

Douglas, D. & Timberg, C. (2014, February 9). Experts warn of coming wave of serious cyber crime. *The Washington Post*. Retrieved on 12th October 2014 from http://www.washingtonpost.com/business/economy/target-breach-could-represent-leading-edge-of-wave-of-serious-cybercrime/2014/02/09/dc8ea02c-8daa-11e3-833c-33098f9e5267_story.html.

Furnell, S. (2002). *Cyber crime: Vandalizing the information society*. London, United Kingdom: Addison Wesley.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social and Legal Studies, 10*(2), 243-249.

Gunter, W. D. (2011). Criminological predictors of digital piracy: A path analysis. In K. Jaishankar (Ed.), *Cyber criminology: Exploring internet crimes and criminal behavior* (p. 173-191).

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

Higgins, G. E. & Makin, D. A. (2004). Does social learning theory condition the effects of low self-control on college students' software piracy? *Journal of Economic Crime Management, 2*, 1-22.

Higgins, G. E. (2004). Can low self-control help with the understanding of the software piracy problem? *Deviant Behavior, 26*(1), 1-24.

Holt, T. J. & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cyber crime victimization. *Deviant Behavior, 30*(1), 1-25.

Holt, T. J. (2010). *Crime on-line: Correlates, causes, and context*. Raleigh, NC: Carolina Academic Press.

Holt, T. J., Bossler, A. M. & May, D. C. (2011). Low self-control, deviant peer association, and juvenile cyberdeviance. *American Journal of Criminal Justice, 37*(3), 378-395. DOI: 10.007/s12103-011-9117-3.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). Social learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice, 33*(2), 31-61.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, 1(1), 1-6.

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmalleger & 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). *Cyber criminology: Exploring Internet crimes and criminal behavior*. Boca Raton, FL: CRC Press.

Jewkes, Y. (2007). *Crime online*. Cullompton, United Kingdom: Willan.

McManus, D. (2014, April 14). Edward Snowden: A whistle-blowing outlaw, now with a Pulitzer Prize to his name. *Los Angeles Times*. Retrieved from 12th October 2014 http://www.latimes.com/opinion/opinion-la/la-ol-pulitzer-prize-edward-snowden-nsa-20140414,0,3959573.story.

Mitra, A. (2003). Cybernetic Space: Our new dwelling place. Proceedings of the Hawaii International Conference on Social Sciences June 12 - 15, 2003. Retrieved on December 20 2006, from www.hicsocial.org/ Social2003Proceedings/AnandaMitra.pdf.

Morris, R. G. & Blackburn, A. G. (2009). Cracking the code: An empirical exploration of social learning theory and computer crime. *Journal of Crime and Justice, 32*(1), 1-34.

Morris, R. G. & Higgins, G. E. (2010). Criminological theory in the digital age: The case of social learning theory and digital piracy. *Journal of Criminal Justice, 38*(4), 470-480.

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

Nhan, J. & Bachmann, M. (2010). Developments in cyber criminology. In M. Maguire & D. Okada (Eds.), *Critical issues of crime and criminal justice: Thought, policy, and practice* (pp. 164-177). Thousand Oaks, CA: Sage.

Patchin, J. W. & Hinduja, S. (2011). Traditional and nontraditional bullying among youth: A test of general strain theory. *Youth and Society, 43*(2), 727-751.

Pati P. (2003) Cyber crime. Retrieved on December 15 2006, from http://www.naavi.org/pati/pati_cyber crimes_dec03.htm.

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*(3), 267-296.

Shaw, Clifford R. & McKay, Henry D. (1942). *Juvenile Delinquency in Urban Areas*. Chicago: University of Chicago Press.

Simpson, S. & Piquero, N. L. (2002). Low self-control, organizational theory, and corporate crime. *Law and Society Review, 36*(3), 509-548.

Smith, R. G., Grabosky, P., & Urbas, G. (2004). *Cyber criminals on trial*. Cambridge: Cambridge University Press.

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

The White House, Office of the Press Secretary. (2009). *Remarks by the President on securing our nation's cyber infrastructure* [Press release]. Retrieved on 12th October 2015 from http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

Thomas, D. & Loader, B. (2000). Introduction. In D. Thomas and B. Loader (Eds.), *Cyber crime: Law enforcement, security and surveillance in the information age* (pp. 1-13). London: Routledge.

United States Department of Justice. Bureau of Justice Statistics. Survey of Inmates in State and Federal Correctional Facilities, 2004. ICPSR04572-v1. Ann Arbor, MI: Inter-university Consortium for Political and Social Research [distributor], 2007-02-28. DOI: 10.3886/ICPSR04572.v1.

United States Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. Survey of Campus Law Enforcement Agencies, 2004-2005: [United States]. ICPSR27261-v1. Ann Arbor, MI: Inter-university Consortium for Political and Social Research [distributor], 2010-03-09. DOI: 10.3886/ICPSR27261.v1.

United States Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. Law Enforcement Management and Administrative Statistics (LEMAS), 2007. ICPSR31161-v1. Ann Arbor, MI: Inter-university Consortium for Political and Social Research [distributor], 2011-07-07. DOI: 10.3886/ICPSR31161.v1.

United States Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. National Crime Victimization Survey, 2012. ICPSR31202-v2. Ann Arbor, MI: Inter-university Consortium for Political and Social Research [distributor], 2013-10-28. DOI: 10.3886/ICPSR34650.v1.

United States Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. National Crime Victimization Survey: Identity Theft Supplement, 2012. ICPSR34735-v1. Ann Arbor, MI: Inter-university Consortium for Political and Social Research [distributor], 2014-02-20. DOI: 10.3886/ICPSR34735.v1.

United States Dept. of Justice, Bureau of Justice Statistics. DIRECTORY OF LAW ENFORCEMENT AGENCIES, 1996: [UNITED STATES]. Conducted by U.S. Dept. of Commerce, Bureau of the Census. ICPSR ed. Ann Arbor, MI: Inter-university Consortium for Political and Social Research [producer and distributor], 1998. DOI: 10.3886/ICPSR02260.v1.

Wall, D. S. (1999). Cyber crimes: New Wine, No Bottles?, in P. Davies, P. Francis and V. Jupp (eds), *Invisible Crimes: Their Victims and their Regulation* (pp. 105-39). London: Macmillan.

Williams, M. (2005) Cyber crime. In J. Mitchell Miller (Ed.) Encyclopaedia of Criminology, London: Routledge.

Yar, M. (2005). The novelty of 'cyber crime': An assessment in light of routine activity theory. *European Journal of Criminology, 2,* 407-427.

Yar, M. (2006). *Cybercrime and society*. London, United Kingdom: Sage.