International Journal of Cyber Criminology
Vol 12 Issue 1 January – June 2018

EDITORIAL

Cyber Criminology as an Academic Discipline: History, Contribution and Impact[1]

K. Jaishankar[2]
International Journal of Cyber Criminology / Raksha Shakti University, India

Introduction

Though, the Internet begun with the introduction of computers in 1950's it was only commercially exploited in the late 1980's. Internet has revolutionized the way in which we see the world. Also, many of the routine, mundane works have been made simple by the advent of the Internet. Especially, e-commerce has changed the patterns of marketing and sales behavior and the banking sector enabled its growth. In addition, the entrance of social media has brought people together. It has cut the boundaries and jurisdictions.

There are many positive uses of the Internet. However, it has become an area of Wild West. Many unscrupulous persons started using it for criminal purposes. Notably, the founding fathers of the Internet did not envisage that it will become a medium of criminality or it will create new forms of crime. Though, Internet is an international space, it is only governed by American laws (Jaishankar, 2011a). This legal lacuna further created problems, as many of the countries did not know how to manage cyber crimes in their jurisdictions.

Initially, academics also could not understand cyber crime as it is a new form of crime (Jaishankar, 2007a). Especially, criminologists were very slow in researching cyber crimes (Jaishankar, 2007a), though; their counterparts in the field of computer and internet science surpassed them and created new fields such as information security and cyber forensics. This gap in the field of criminology was well addressed by me and I founded the academic discipline "Cyber Criminology" in the year, 2007. Recently, Ndubueze (2017, p, 17) and Meško (2018, p. 190) formally credited me as the Founding Father of Cyber Criminology.

---

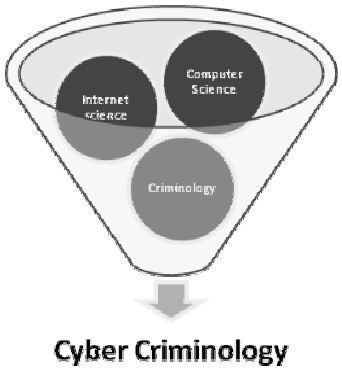
[1] Founding Father of Cyber Criminology; Founding Publisher and Editor-in-Chief, International Journal of Cyber Criminology; Professor and Head, Department of Criminology, Raksha Shakti University, Ahmedabad, Gujarat, India. Url: www.jaishankar.org

[2] Earlier, published as a part of the E-PG Pathsala Criminology, UGC-MHRD as a module in the Paper, Cyber Criminology and Cyber Forensics. Principal Investigator - G. S. Bajpai, Paper Coordinator - K. Jaishankar (Cyber Criminology and Cyber Forensics).
Shared here under the terms of Creative Commons Attribution - ShareAlike, CC-BY licence https://creativecommons.org/licenses/by-sa/4.0/

1. History, Evolution and Definition

Cyber space has been exploited by many fields of study; however, criminology was too late to explore this space and address the new form of criminality called cyber crime. I addressed the causation of cyber crime and found a new academic sub-discipline of Criminology called "Cyber Criminology" in 2007, with the launch of a journal; the International Journal of Cyber Criminology (www.cybercrimejournal.com). I academically coined the term "Cyber Criminology" and defined cyber criminology as *"the study of causation of crimes that occur in the cyberspace and its impact in the physical space"* (Jaishankar, 2007a, para 1).

Figure 1



Source: P. Madhava Soma Sundaram, & Syed Umarhathab (2011a) p. xxi

As an academic discipline, cyber criminology encompasses multidisciplinary field of inquiry - criminology, sociology, psychology, victimology, information technology and computer / internet 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, 2011b; Ngo & Jaishankar, 2017, p. 4). I created this new field within the larger ambit of criminology for two main reasons. "First, the body of knowledge that deals with cyber crimes should not be confused with investigation and be merged with cyber forensics; second, there should be an independent discipline to study and explore cyber crimes from a social science perspective" (Jaishankar, 2010, p. 26).

Now, the discipline of cyber criminology is more than ten years old and it has successfully entered the portals of academia in the form of courses starting from minor/major courses (University of Alabama, Regis University, Saint Anselm College and Purdue University, USA offer a minor in Cyber Criminology and Florida State University, USA offers a major in Cyber Criminology) to bachelor of science (B.S.) in cyber criminology and security studies (Indiana State University, USA) and Associates in Arts (A.A) Degree in Cyber Criminology (at Arizona Western College, USA). Many of the Universities in the United States have recruited Assistant Professors in the field of Cyber Criminology. Also, many doctoral researchers are involved in research on Cyber Criminology.

2. Contribution and Impact

Though the field of cyber criminology has many contributions and it has immense impact, only two of the major contributions and its impact are discussed here. They are: *a. International Journal of Cyber Criminology and b. Space Transition Theory of Cyber Crimes.*

a. International Journal of Cyber Criminology: A Journal nonpareil for the advancement of the field of Cyber Criminology

Cyber Criminology as an academic sub-discipline of criminology was born with the launch of the International Journal of Cyber Criminology (ISSN: 0974 – 2891, www.cybercrimejournal.com), by me in 2007. This multidisciplinary journal is published "biannually and devoted to the study of cyber crime, cyber criminal behavior, cyber victims, cyber laws and cyber policy" (Jaishankar, 2007a, 2010). This journal is solely dedicated to the publication of papers purely from social science perspective of cyber crimes. However, some moderate technical articles are also accepted for publication in this journal when they have an aim to advance cyber policy to prevent cyber crimes. The International Journal of Cyber Criminology is a unique open access journal. This journal follows the Diamond open access policy. Unlike many other open access journals which charge heavily on their authors, the International Journal of Cyber Criminology does not charge its authors or the readers as this journal believes in social justice and it is free to anyone who has an access to the internet.

This journal is indexed in several prestigious databases. Scopus and Directory of Open Access Journals (DOAJ) are some of the prestigious databases that have included this journal. The Scopus reviewers' have highly commended this journal for its inclusion in the Scopus database: "*The papers published here are well-done and reasonably well cited, so, I am recommending that the journal be accepted for inclusion in Scopus*" (on personal communication to the Editor-in-Chief, Professor K. Jaishankar). This journal is currently under the consideration for Journal Impact Factor of the Clarivate Analytics (Already indexed in Emerging Sources Citation Index). This journal presently follows Hirsch's h-index for Journal impact and the current h-index is 30 and the 2017 Cite Score of Scopus is 2.00. The International Journal of Cyber Criminology has improved the Cite Score of Scopus from 0.45 (2013) to 2.00 (2017) and improved in ranking from 202nd position (out of 548 criminology journals) to 36th position. The International Journal of Cyber Criminology is also listed as an essential or additional reading in several cyber crime courses across the world. Also, recently (2017), the University Grants Commission (UGC) India, has listed the International Journal of Cyber Criminology in its approved list of journals.

Notably, the International Journal of Cyber Criminology is reviewed by Cheryl LaGuardia, Research Librarian, Widener Library, Harvard University, USA for the Magazines for Libraries, ProQuest LLC, USA. She opines: The Journal "material comes from authors around the world, and is heavily referenced and targeted for academic use. The journal is indexed in Criminal Justice Abstracts and SCOPUS and will be of interest to theoretical researchers in cyber crime and Internet-based criminality" (2016, para 2). Also, in 2011, I brought out a special edited volume (a book) of selective articles of the International Journal of Cyber Criminology and it is titled as *"Cyber Criminology: Exploring Internet Crimes and Criminal Behavior"* and it published by CRC Press, Taylor and Francis Group, USA.

Ten Years back, Bachmann (2008) asserted: "the strongest indicator of the … establishment of cyber criminology as a distinct subsection within criminology is that the

first interdisciplinary research journal dealing exclusively with cybercrime, the International Journal of Cyber Criminology, was first published in January 2007… by Jaishankar". The International Journal of Cyber Criminology is now commemorating its decade of existence and has reached its aim to become a "nodal centre to develop and disseminate the knowledge of cyber crimes to the academic and lay world," from a social science perspective.

b. Space Transition Theory of Cyber Crimes: A unique Theory to further the discipline of Cyber Criminology

There are many scholars who attempted to address the causation of cyber crimes with traditional theories such as Social Learning Theory, Routine Activities Theory and Drift and Neutralization theory. However, they were not fully successful in their explanation of cyber crimes, as the cyber space is altogether a new space and cyber crime is a new form of crime (Yar, 2005; Jaishankar, 2007b, 2015). The Space Transition Theory of Cyber Crimes (2008) was propounded by me because I found that there is no theory that is specifically created to address the causation of cyber criminality. I first presented this theory at the John Jay College of Criminal Justice, The City University of New York, USA, in 2007. Later, I published this theory as a chapter in a book titled "*Crimes of the Internet*" edited by Frank Schmalleger and Michael Pittaro (2008), and published by Prentice Hall, USA.

The Space Transition Theory of Cyber Crimes (2008) advances the field of Cyber Criminology. "Space Transition Theory" is an explanation about the nature of the behavior of the persons who bring out their conforming and non-conforming behavior in the physical space and cyber space (Jaishankar, 2008, pp. 292-296). Space Transition Theory argues that, people behave differently when they move from one space to another" (Jaishankar, 2008, pp. 292-296). For a detailed discussion on the theory please see Schmalleger and Pittaro (2008).

3. Appreciation

Bachmann (2008) emphasized that the growth of the field of cyber criminology is seen by two strong indicators. One, the launch of the exclusive journal, the International Journal of Cyber criminology in 2007 and two, the significant growth of scholarly publications in the form of books, journal articles and book reviews in the area of cyber crime/cyber criminology in the past ten years of the establishment of the field of cyber criminology by me. Moore (2010) has dedicated a chapter on "Cyber Criminology" in his book titled *"Cybercrime Investigating High-Technology Computer Crime"*. Stalans and Finn (2016, pp. 502-503) values: "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, 2011b; Kshetri, 2013; Wall, 2007) and *Twelve* (emphasis mine) reviews on the current state of knowledge" (Bachmann, 2008; Choi, 2015; Diamond & Bachmann, 2015; França, 2018; Holt & Bossler, 2014, 2016; Jahankhani, 2018; Maras, 2016; Ndubueze, 2017; Nhan & Bachmann, 2010; Ngo & Jaishankar, 2017; Stalans & Finn, 2016).

4. Challenges

There are many challenges in the establishment of an academic discipline such as Cyber Criminology. Jaishankar (2010, p. 27) has identified three challenges (a) issues in teaching, (b) research in cyber criminology, and (c) professionalization of the discipline. Later, in 2015, Diamond and Bachmann identified one more challenge, i.e., d) Marginalization by mainstream Criminology.

(a) Issues in Teaching

The contemporary teaching of cyber crimes is separately done by cyber security/forensics specialists, cyber lawyers and cyber criminologists. Jaishankar (2010) feels that current teaching in cyber criminology is compartmentalized and will be of no use. He laments that this compartmentalized teaching will stunt the growth of fields of cyber criminology and also cyber forensics/security, as professionals will be developed only with lopsided knowledge of cyber crimes. Further, he recommends for a holistic teaching, where the curriculum should be a blend of social science, law and technology. He emphasized the "strong need for holistic professionals who have a collective knowledge of cyber criminology, law, and forensics and who can take cyber criminology to the next level (Jaishankar, 2010, p. 27).

(b) Research in Cyber Criminology

In the post establishment period of Cyber Criminology (2007) research in this field has advanced. There are now several journal and book publications in this field. The papers published in the International Journal of Cyber Criminology serves as a great repository to the field of Cyber Criminology. However, due to lack of data, empirical research in this field has not enhanced. Though, it is easy by cyber criminologists to identify victims of cyber crimes, it is difficult for them to get offender samples. Hence, with minimum sample size of cyber offenders, only theoretical/qualitative research is done. This is one of the significant challenges which need to be addressed by the future cyber criminologists. However, surplus empirical research (Qualitative and Quantitative) are done in the area of cyber victimization. This also has paved way for the creation of cyber victimization theories such as "Irrational Coping Theory of Cyber Victimization" (Halder & Jaishankar, 2015) and a *new sub-field* "Cyber Victimology", defined by Jaishankar (2015) as "*the study of forms of online victimization, its impact on victims, and responses of society and systems*" (*found by me in 2015 – presented at the 15th World Society of Victimology Symposium, July 5-9, 2015, at Perth, Australia*) and further being developed as a Book (Jaishankar & Halder, forthcoming).

(c) Professionalization of the Discipline

Creation of jobs is one of the major challenges that cyber criminology face. To meet this challenge, cyber criminology needs to include more practicals in the curriculum. Mere theoretical approach will not develop holistic professionals. "The amalgamation of cyber criminology, laws, and computer forensics can pave a new pathway for new jobs in the field of cyber criminology" (Jaishankar, 2010, p. 28)

d) Marginalization by mainstream Criminology

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; Ngo & Jaishankar, 2017, p. 5). There may be a symbolic reason for the neglect of cyber criminology by the mainstream criminology. Most of the conventional criminologists are digital immigrants (people born before 1985 and have adopted digital technology later) and barring a few, many are not interested to address the issue of cyber crime, as they endure generation gap problems. Except a handful of researchers (they are digital immigrants), many have not ventured in to the field of cyber criminology nor do they profess this field or acknowledge cyber criminology as a distinct discipline. Also, some of the cyber criminologists feel that conventional criminologists are not knowledgeable or have expertise in fields such as cyber forensics and information security or cyber policy (Holt, Bossler & Spellar, 2015) and they feel that criminologists only look "cyber crime from a sociological perspective" (Holt, Bossler & Spellar, 2015, p. 309). However, in the near future, this challenge will be met by the Digital Natives (*a term coined by Marc Prensky (2001), meaning, people born during or after the rise of digital technologies*). The digital native cyber criminologists will understand the technology better than the digital immigrant criminologists and they will have a multi-disciplinary approach and will take the discipline of cyber criminology to greater heights.

Conclusion

The growth of the field of Cyber Criminology is imperative as there is a surge of cyber crimes in the past decade. Ngo and Jaishankar (2017, p. 5) feels that: "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)." Moore (2012, p. 283) feels that: "There is no denying that this area of criminology (cyber criminology) is extremely exciting and certain to become a well-researched area of criminal behavior". It is envisaged that the field of cyber criminology will grow to a greater extent and there will be no more neglect or marginalization of mainstream criminology. "More so, the discipline of cyber criminology will remain central to the search for answers to the astounding questions of law and order in the twenty-first century cyber space" (Ndubueze, 2017, p. 70).

Acknowledgement

I sincerely thank Ms. Leepaxi Gupta, the new Editorial Assistant of the International Journal of Cyber Criminology (IJCC), for significantly assisting me in formatting and copyediting the articles. She was burning the midnight oil to finish the formatting work of this issue. The Editorial Board of IJCC offers its earnest thanks to her.

References

Bachmann, M. (2008). What makes them Click? Applying the rational choice perspective to the hacking underground. Doctoral Dissertation Submitted to the University of Central Florida. Retrieved from http://etd.fcla.edu/CF/CFE0002258/Bachmann_Michael_200807_PhD.pdf.

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

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

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.

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. (2016). *Cyber crime in Progress: Theory and Prevention of Technology-enabled Offenses*. Abingdon, Oxon: Routledge.

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

Jahankhani, H. (Ed.) (2018). *Cyber Criminology*. Springer Nature Switzerland AG: Springer International Publishing.

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

Jaishankar, K. (2007b). Establishing a theory of cyber crimes. *International Journal of Cyber Criminology, 1*(2), 7-9.

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

Jaishankar, K. (2011a). Epilogue: Raising the Human Spirit and Restoring Order in the Information Super Highway. In: P. Madhava Soma Sundaram, & Syed Umarhathab. (Ed.), Cyber Crime and Digital Disorder (pp. 149-153). Tirunelveli, India: Publication Division, Manonmaniam Sundaranar University.

Jaishankar, K. (2011b). 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*. London: Routledge. ISBN: 978-14-987848-9-4.

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

LaGuardia, C. (2016). Review of International Journal of Cyber Criminology. Retrieved from http://www.proquest.com/blog/mfl/2016/International-Journal-of-Cyber-Criminology.html.

Madhava Soma Sundaram, P., & Umarhathab, S. (2011). Editors' Introduction: From Cipher Knowledge to Cyber Knowledge …The Rise of Technology and the fall of Human Sprit. In P. Madhava Soma Sundaram, & Syed Umarhathab. (Eds.), *Cyber Crime and Digital Disorder* (pp. xvii-xxviii). Tirunelveli, India: Publication Division, Manonmaniam Sundaranar University.

Maras, M. H. (2016). *Cybercriminology*. Oxford: Oxford University Press.

Meško, G. (2018). On Some Aspects of Cybercrime and Cybervictimization. *European Journal of Crime, Criminal Law and Criminal Justice*, *26*(3), 189 – 199. DOI: 10.1163/15718174-02603006

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

Ndubueze, P. N. (Ed.). (2017). *Cyber Criminology and Technology-Assisted Crime Control: A Reader*. Nigeria: Ahmadu Bello University Press Ltd.

Ngo, F., & Jaishankar, K. (2017). Special article: Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime. *International Journal of Cyber Criminology, 11*(1), 1–9. http://doi.org/10.5281/zenodo.495762.

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.

Prensky, M. (2001). Digital Natives, Digital Immigrants. From On the Horizon. MCB University Press, 9(5), October 2001. Retrieved from http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf.

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

Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427. DOI: 10.1177/147737080556056.