EDITORIAL

The Future of Cyber Criminology: Challenges and Opportunities[1]

K. Jaishankar

Internet technology and the development of cyberspace have taken society to the next level of evolution. Cyberspace has defied the boundaries and has made geography (or place) irrelevant. Cyberspace presents myriad potential opportunities for society in the new millennium. In the 1990s, a new era was ushered in, in which Internet technology reigned supreme. However, the increase in the netizens has dwarfed the technology to a mere medium. Additionally, the perpetrators who attacked machines through machines have started attacking real humans through the machines. This radical development led criminologists to address the need for a discipline to study and analyze criminal behavior in cyberspace. The crimes, offender behaviors, and victimization that occur in cyberspace needed to be studied from a social science versus a technological perspective. In this backdrop, I established cyber criminology as a sub discipline within the larger ambit of Criminology in 2007, with the launch of the International Journal of Cyber Criminology (http://www.cybercrimejournal.com), an online open access journal. In 2008, I also developed a theory to further the discipline of cyber criminology. The theory is called space transition theory, and it explains the causation of crimes in cyberspace (Jaishankar, 2007, 2008).

Cyber criminology is a multidisciplinary field that encompasses researchers from various fields such as criminology, victimology, sociology, Internet science, and computer science. I define cyber criminology as "the study of causation of crimes that occur in the cyberspace and its impact in the physical space" (Jaishankar, 2007, para 1). I academically coined the term cyber criminology for two 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.

Since the launch of the International Journal of Cyber Criminology, the term cyber criminology has taken its academic roots in the online as well as offline academic circles (Jaishankar, 2007; Nhan & Bachmann, 2010). According to Nhan and Bachmann (2010), "Cyber criminology is slowly emerging from a niche area that is often marginalized by mainstream criminology to one of high importance" (p. 175). Although cyber criminology is gaining hold within the mainstream field of criminology, the big question is, "Will it evolve as a separate discipline?" There are many such criminologies that have

[1] Copyright © 2011. From *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* by K. Jaishankar. Reproduced by permission of Taylor and Francis Group, LLC, a division of Informa plc.

not become separate disciplines (e.g., green criminology, bio-criminology, environmental criminology). One reason could be that in spite of their research scope, they lacked content that could be taught. However, cyber criminology has the potential to become an independent discipline because of its dynamic expansion of exceptional interdisciplinary content in teaching and research.

If cyber criminology is to be established as a separate discipline, various challenges face the modern-day cyber criminologists. These challenges include (a) issues in teaching, (b) research in cyber criminology, and (c) professionalization of the discipline.

1. Issues in Teaching

Many of the universities in the United States and the United Kingdom offer criminology programs with a course in cyber crime. Recently, some universities in the United Kingdom—such as Canterbury Christ Church University; University College, Dublin; and University of Bedfordshire—have started offering master of science (MSc) courses in cyber crime forensics and forensic computing. The mushrooming courses on cyber forensics prove that universities are more interested in the practical investigative part of cyber crimes than the causation of cyber crimes. Although the practical part is important, neglecting the theoretical issues behind cyber crimes would not compliment a holistic understanding of cyber crimes. Hence, courses should be offered as an MSc in cyber criminology and forensics; this will enable a combination of both theoretical and practical aspects of cyber crimes.

Getting quality teachers to teach cyber crimes, laws, and investigation is one of the biggest challenges in developing programs in cyber criminology. The growth of Internet science, computer science, and information technology has a great impact on the development of the cyber criminology discipline. Conventional criminologists do not seem to be adapting to the growing needs of the expanding criminological discipline. They are not learning additional disciplines such as information technology and Internet science, both of which encompass the scope of cyber criminology. Without technical knowledge, conventional criminologists cannot move beyond teaching the merely theoretical aspects of cyber crime. On the other hand, if technocrats were to be involved in teaching cyber criminology, they may be much less concerned with teaching the fundamentals of cyber criminology. They might be more inclined to speak about the technology than about the issues behind the cause of cyber crimes. Alternatively, if lawyers were to teach cyber criminology, they might focus only on cyber laws, thus leaving out other important components of cyber crimes. Such atomistic teaching by criminologists, technocrats, or lawyers will not help efforts to advance the formal discipline of cyber criminology. There is a 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. Conventional criminology departments could offer a multidisciplinary program of cyber criminology and forensics with assistance from other departments, such as departments of computer science, law, and information technology. Those professionals who complete their degrees in cyber criminology could then be further absorbed as research and teaching assistants to develop the discipline. This would create a pool of professionals who would serve as a repository, of sorts, with a blend of both theoretical and practical knowledge of cyber crimes, investigation, and laws; these professionals would be valuable in advancing the profession as well as assisting the criminal justice administration in the investigation of cyber crimes.

2. Research in Cyber Criminology

Current research in cyber criminology is highly encouraging. New and old criminologists have quickly understood the gap in research that has occurred in the areas of cyber crime research (Nhan & Bachmann, 2010). Even though phase of research is slow in this area, it is gaining momentum (Jewkes, 2006; Mann & Sutton, 1998). There are now also a handful of edited collections and authored books on cyber crimes written by criminologists purely from criminological perspectives (Jewkes, 2007; McQuade, 2005; Schmalleger & Pittaro, 2008; Smith, Grabosky, & Urbas, 2004; Wall, 2001, 2003, 2007, 2009; Yar, 2006; Yar & Jewkes, 2010). Research Articles published in the International Journal of Cyber Criminology are qualitative and quantitative and of high quality.

Because research in cyber criminology is new, it is not devoid of its own methodological flaws. In their recent work, Nhan and Bachmann (2010) highlighted certain methodological errors in cyber crime research. They feel that the "lack of a general definition, measurement issues, and survey problems such as bias and errors" (pp. 179 – 182) must be rectified by cyber criminologists in the future. Apart from these research issues, there is a dearth of researchers in the field of cyber criminology. Except for a few researchers in countries that include the United States, the United Kingdom, India, and Canada, there are no major researchers working in the field of cyber criminology. As pointed out earlier in the Issues in Teaching subsection, these lacunae can be overcome by creating more cyber criminologists. Research collaboration among various universities that conduct work in the field of cyber criminology can also fill this gap. Additionally, constant visits to the research centers by professionals from the industry would help in the development of research collaboration and transfer of expertise.

3. Professionalization of the Discipline

The major challenge that a new field of cyber criminology would face is the issue of the creation of jobs and the professionalization of the discipline. If cyber criminology remains a theoretical discipline, the creation of jobs would remain only at the level of theoretical research. As emphasized earlier, there is a need to grow cyber criminology as not only a theoretical but also a practical discipline. The amalgamation of cyber criminology, laws, and computer forensics can pave a new pathway for new jobs in the field of cyber criminology. Various universities and other bodies can create a certification program for cyber criminologists. These cyber criminologists can assist the police departments in the investigation of cyber crimes and start their own companies. Cyber criminologists also can evolve as cyber law specialists. Another significant area to which cyber criminologists can contribute is victim services. Cyber criminologists can become cyber victim counselors, who would counsel individuals who have fallen prey to cyber crimes and advise corporate bodies in the prevention of cyber victimization. Cyber criminologists also could act as a resource center on cyber crime victimization that would create awareness among the scholarly and lay public.

Opportunities

The installation of a new International Cyber Crime Research Centre at the Simon Frazer University Centre for Cybercrime Research and at the University of Ontario Institute of Technology—both in Canada—provides a good base for the development of research works in cyber criminology. Research centers such the Berkman Center for Internet and Society and the Centre for Cybercrime Studies at John Jay College of

Criminal Justice are dedicated to contributing to the growth of cyber criminology. A cursory search on the Internet provides information about more such centers that are being developed and launched. This information gives me great hope that research in cyber criminology will be taken in an entirely new and exciting direction.

Also, I sincerely believe that the challenges discussed herein can be overcome by current and future cyber criminologists, and I see a bright prospect for the growth of cyber criminology as an independent discipline.

About the current issue

This issue is a combined issue of volume 4 (Issue 1 & 2). This consists of an editorial, eight articles and a book review.

Elena et al in their article bring out a hitherto unexplored phenomenon, the online child sexual abuse by the female offenders. Though child sexual abuse is mostly considered as a crime committed by men, females too involve in such crimes, though not reported frequently. The anonymity of internet further helps female offenders to hide and abuse innocent children. Elena et al also emphasizes that this crime is committed with the assistance of male colleagues and during investigation used the techniques of neutralization was utilized by the female offenders. Though an in depth analysis in to the minds of female offenders is not done (which is difficult at the present moment), this article is a significant contribution to the field of cyber criminology as it has started looking child sexual abuse from a gendered perspective.

Hu et al from the fields of finance and communication has provided a novel contribution to cyber criminology. Their in-depth analysis of spams moves in a new direction. They have analyzed the trading behavior of individuals vis a vis spams sent to them by the stock marketing companies. They analyzed over 40,000 spam messages and found "abnormal returns, trading volume, and intraday price volatility were significantly higher for spam e-mails containing a target price". Their analysis also found that mostly the firms that had a headquarters outside US have less target value than the firms that had headquartered in US. This may be an issue of trustworthiness among the minds of the users in connection with the stock markets.

Marion Dion has analyzed advanced fee fraud letters from a Machiavelian/narcissistic perspective. Dion further explores the nuances in these letters and how they utilize the skills of marketing to defraud the victims by emphasizing that they hail from a glorious background and the victim is privileged of such contact. This article is a key qualitative contribution as this has added color to the analysis of advanced fee fraud letters. This article has looked in to the psyche of the offenders who write such letters from a different angle and that make this a noteworthy contribution.

As the cyberspace is elusive, it is very difficult to undertake a study of offenders. *Bachmann* in his article has made an attempt to analyze the risk propensity of hackers. Contacting hackers is not an easy task and Bachmann needs to be congratulated for undertaking such a painstaking study. Bachmann's study tries to analyze the psyche of the hackers and found that hackers take more risk than others and this makes them different from the common masses. He also tried to analyze such behavior with some theories of crime. As this is an exploratory study, an extensive corroboration with such theories was not possible. This article fills in the gap of literature of cyber criminology, especially in the area of cyber offenders.

Music piracy is a highly debatable area. Many countries in the world differ in the ownership of music. While some countries strongly emphasize the copyright issue and ownership of music, some countries openly allow download of music via torrents and other peer to peer sites. *Gunter et al* explores this aspect from a different set of population from an US perspective. As most of the studies in this area so far concentrated among college students, this study comes as a break in the tradition. This study analyzed the behavior of music piracy among school students. The researchers tried to "predict involvement in music piracy with demographics (sex, race, and class), educational achievement and aspirations, and self-control" and found that the said factors had an effect on the school students in relation with music piracy.

Cyber bullying is one of the largest analyzed crimes of the internet. However, cyber bullying research remains only to populations of few countries. *Su and Holt* have moved beyond this convention and have analyzed a set of population which was not studied earlier. They examined the behavior of victims and bullies of a Chinese population. Until now, language barrier did not allow such studies to be brought to the international audience. However, with efficient translators and analysts such studies became possible and this study is an important contribution as it gives a new dimension to cyber bullying research. The study found out the usage of sexual overtones in bullying and also the concern of the bystander towards victims. This finding of bystander support is very new as most of the other studies have shown the involvement of bystander as either an active or passive participant and not as a strong mediator who stop such crimes.

Reporting behavior is an important area of research in the field of victimology. *Moore et al* have tried to examine the reporting behavior of online harassment. Unlike the physical space harassment where females tend not to report their victimization, most of the females have reported their online victimization. The researchers have also found that parental regulations had no impact on their reporting behavior. Also the researchers emphasized that youth who are more in the cyberspace report more on their victimization than those who infrequently visit the cyberspace. This research on cyber victimization fills the gap in the literature and is a novel contribution to both the fields of cyber criminology and victimology.

The analysis by *Marion* is on the effectiveness of the Convention of Cyber Crime created by the Council of Europe in 2001. Marion examines the Convention of Cyber Crime from the symbolic perspective developed by Edelman (1964). She has made a extraordinary critique of the Convention of Cyber Crime and emphasized that the current stature of the Convention of Cyber Crime is not going to be useful to member countries in the mitigation of crimes, as it is a mere symbolic exercise. She has also provided some suggestions to improve the effectiveness of the Convention of Cyber Crime and for creating better policy on cyber crimes.

Acknowledgements

This issue was possible only because of the authors continued faith in the quality of the International Journal of Cyber Criminology and its outstanding reviewers. The reviewers of this issue provided their review in a short notice and have greatly supported me in bringing out the issue. From the bottom of my heart, I sincerely thank all the reviewers for their constant support and assistance that makes International Journal of Cyber Criminology a quality online open access journal which sincerely believes that knowledge of cyber crimes should unreservedly reach everyone who has an access to the internet.

References

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

Jaishankar, K. (2007). Editorial: Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology*, *1*(2), 7–9.

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.

Jewkes, Y. (2006). Comment on the book Cyber Crime and Society by Majid Yar, Sage Publications. Retrieved on 15th April 2010 rom http://www.sagepub.co.uk/booksProdDesc. nav?prodId=Book227351

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

Jewkes, Y., & Yar, M. (2010). *Handbook of Internet crime*. Cullompton: Willan

Mann, D., & Sutton, M. (1999). NetCrime. More change in the organisation of thieving. *British Journal of Criminology*, *38*(2), 201-229.

McQuade, S. C. (2005). *Understanding and managing cyber crime*. Upper Saddle River, NJ: Allyn & Bacon.

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.

Schmalleger, F., & Pittaro, M. (Eds.) (2008). *Crimes of the Internet*. Upper Saddle River, NJ: Prentice Hall.

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

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Cambridge, UK: Polity.

Wall, D. S. (Ed.). (2001). *Crime and the Internet*. London: Routledge.

Wall, D. S. (Ed.). (2003). *Cyberspace crime*. Aldershot, UK: Dartmouth/Ashgate (Dartmouth International Library of Criminology and Penology).

Wall, D. S. (Ed.). (2009). *Crime and deviance in cyberspace*. Aldershot, UK: Dartmouth/ Ashgate (Dartmouth International Library of Criminology and Penology).

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