

## EDITORIAL

### Cyber Criminology: Evolving a novel discipline with a new journal

**K. Jaishankar**

Cyberspace presents an exciting new frontier for criminologists. Virtual reality and computer mediated communications challenge the traditional discourse of criminology, introducing new forms of deviance, crime, and social control (McKenzie 1996). Since the 1990s, academics have observed how the cyberspace has emerged as a new locus of criminal activity (Thomas and Loader 2000; Littlewood 2003; Yar 2005), but in general, criminology has been remiss in its research into the phenomena of cyber crime and has been slow to recognize the importance of cyberspace in changing the nature and scope of offending and victimization (Mann and Sutton 1998; Jewkes 2006). A new, radical discipline named cyber criminology is the need of the hour to explain and analyze the crimes in the internet. The field of cyber criminology crystallizes for many Scientists and Social scientists an area of research at the interface between Computer Science, Internet Science and Criminology. I define cyber criminology as *"the study of causation of crimes that occur in the cyberspace and its impact in the physical space"*.

For a year or so, the word cyber criminology has slowly appeared in the internet. Also, McAfee has used an alternate word "Virtual Criminology" in their report published in 2006. The first conference devoted entirely to this area was the "Cyber Criminology and Digital Forensics Initiative Conference" which took place in Spokane Valley, WA, USA in October 2006. This was also a new direction to segregate cyber-forensics and cyber criminology. Quite often, cyber criminology is merged with cyber-forensics. There is a need to identify the differences between cyber criminology and cyber-forensics. Cyber-forensics deals exclusively with the investigation of cyber crimes, whereas, cyber criminology deals with the causation of cyber crimes.

## Why we need a journal for Cyber Criminology?

As the discipline of cyber criminology approaches the future, facing the dire need to document the literature in this rapidly changing area has become more important than ever before. Although we have all recognized the importance of interdisciplinary research, the fields of Internet Science, Computer Science and Criminology have remained compartmentalized. Collaboration is still difficult since the language of these disciplines is different. Moreover, the scientific journals in these fields are also clearly separate. Researchers involved in cyber criminology have a choice of publishing their research in either computer science-oriented journals or criminology journals. With exception from the Journal of Digital forensic practice and International Journal of Electronic Security & Digital Forensics which exclusively focuses on practical issues of cyber crimes, there is no journal currently available for the interdisciplinary field of cyber criminology. In order to capitalize on the potential of cyber criminology, it is necessary to break down the traditional barriers between Internet scientists, Computer Scientists and Criminologists not just in the laboratory but also in the publication of scientific papers.

We do, therefore, need a new journal that provides a platform for this emerging interdisciplinary field of cyber criminology where Internet scientists, Computer scientists, communication specialists and criminologists can publish their work in one periodical that spans the disciplines. International Journal of Cyber Criminology (IJCC) will provide this platform. The new journal will publish full-length articles of the highest quality and importance in the field cyber criminology. The scope of International Journal of cyber criminology encompasses empirical and theoretical aspects of cybercrime, cyber criminal behavior, cyber victims, cyber laws and cyber investigations. The scope of the journal has both depth and breadth in areas relevant to the interface between Internet Science, Computer Science and Criminology. Experts in the areas encompassed by the journal's scope have been identified for the Editorial Advisory Board and the composition of the board will be continually updated to address the developments in this new and exciting field. The IJCC will be a nodal centre to develop and disseminate the knowledge of cyber crimes to the academic and lay world.

## The First Issue of the Journal

The first issue of this new journal covers a variety of topics: Computer Crime Investigation, Internet Gambling, Cyber Bullying, Digital piracy and Email Fraud. The first issue has five articles and two book reviews. The first issue indicates the type of journal we hope to become. It is wide ranging and inter-generational. Our contributors include scholars at every stage of their academic career, from graduate students to some of the pioneers in the field of cyber criminology. All articles have been reviewed by one or more disciplinary specialists, and all have been revised in light of their expert commentary.

Computer crimes are requiring law enforcement departments in general and criminal investigators in particular to tailor an increasing amount of their efforts toward successfully identifying, apprehending, and assisting in the successful prosecution of perpetrators. *“Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future”*, by Hinduja, outlines the key research findings in the area of traditional American criminal investigations. Similarities and differences between traditional and computer crime investigations are presented and consequent inferences are discussed. This paper also focuses on practical ideas on how the American computer crime investigative task forces can most competently fulfill their intended objectives, by a hypothetical example of a specialized unit.

The status of Internet gambling on the world scene has been notably addressed in the David and Goliath dispute between the United States and the small Caribbean islands of Antigua and Barbuda, which constitute a single nation. *“Offshore internet gambling and the world trade organization: Is it criminal behavior or a commodity?”*, by Pontell, Geis and Brown discuss the dispute represented by the first attempt of the World Trade Organization (WTO) to examine cross-border electronic services, with the added ingredient that the behavior itself, under review has at certain times and in certain places been regarded as criminal. This paper attempts to trace the development of the WTO case offering a view of what is regarded as the most sensible and probably the inevitable path that the trajectory of internet gambling should and will take.

Higgins examines the links between low self-control, rational choice, value, and digital piracy in his study entitled, *"Digital Piracy, Self-Control Theory, and Rational Choice: An Examination of the Role of Value"* To date, several researchers had shown that attitudes, low self-control, social learning theory and deterrence theory to explain digital piracy. No study has examined whether the rational choice theory mediated the link between low self-control and digital piracy. Also no research in digital piracy or criminological literature had considered the role of value in such an examination. This study, built on the mediating model presented by Piquero and Tibbetts (1996), reasons how the rational choice theory establishes the link between low self-control and digital piracy.

Cyber bullying is a psychologically devastating form of social cruelty among adolescents. Shariff and Hoff in their study, *"Cyber bullying: Clarifying Legal Boundaries for School Supervision in Cyberspace"*, review the current policy vacuum of the legal obligations and expectations of schools to monitor and supervise online discourse, while balancing student safety, education, and interaction in virtual space, which also encompasses a discussion of the institutional responses to cyberbullying. An emerging and established law is highlighted to provide guidelines to help schools reduce cyberbullying through educational means that protect students and avoid litigation.

In the study, *"A Qualitative Analysis of Advance Fee Fraud E-mail Schemes"*, Holt and Graves discuss the implications of this study for law enforcement and computer security, exploring the mechanisms that are employed by scammers through a qualitative analysis of 412 fraudulent e-mail messages. Criminals utilize the Internet to perpetrate all manner of fraud, with the largest dollar losses attributed to advance fee fraud e-mail messages. Half of all the messages also request that the recipient forward their personal information to the sender, thereby enabling identity theft. The findings demonstrate that multiple writing techniques are used to generate responses and information from victims.

Marcum reviews, *"Sexual Predators: How to Recognize Them on the Internet and on the Street - How to Keep Your Kids Away"*; a book by the award-winning, investigative journalist Stephen Dean. Dean has had years of experience working with authorities investigating crimes against children. His work has been featured on ABC, NBC, CBS and CNN, as

well as many local news stations. Marcum evaluates how this book attempts to educate parents of the dangers online and what we can do as responsible adults to keep our children safe. In conclusion, she suggests that despite its limitations, this book would be an excellent read for a student of criminology and/or information systems.

In another review, Pierce, describes how J.A. Hitchcock, one of America' leading authority on cyber crime, comprehends the limitations of technical knowledge of the average computer user in the second edition of her book, "Net crimes & misdemeanors: Outmaneuvering webspammers, stalkers and con artists". Her revised edition explains various types of Internet and computer based crimes, and provides definitions and tips applicable to the novice and experienced computer user. Hitchcock has taught various college level courses, written for magazines and newspapers, gives lectures, appears on television and radio and trains law enforcement on how to track cyber criminals and provide assistance to victims.

### **Acknowledgements**

I am grateful to Susan Brenner who has agreed to be the Chief Editorial Advisor and Shaheen Shariff for agreeing to be the Book review Editor of the journal. I am also grateful to Serials Publications, New Delhi and Mr. Vijaya kumar in particular for putting together this new journal to accommodate the fast-growing field of cyber criminology. T. Samyuktha, the editorial assistant of the journal played a vital role in assisting me in proof reading the articles and formatting it for the web, my earnest thanks go to her. I thank all the Editorial Advisory board members who shared their valuable time in peer reviewing the articles and submitting them in time which enabled me to launch the journal in January 2007 as promised earlier in the call for papers. Last but not the least, my sincere thanks goes to the authors for their interest in publishing with the International Journal of Cyber Criminology.

Regards,

**K. Jaishankar**  
Editor-in-Chief

## References

- Adamski A. (1998) Crimes Related to the Computer Network. Threats and Opportunities: A Criminological Perspective. Helsinki, Finland: European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI). Retrieved on December 15 2006, from <http://www.ulapland.fi/home/oiffi/enlist/resources/HeuniWeb.htm>
- Jewkes Yvonne (2006). Comment on the book 'Cyber crime and Society by Majid Yar, Sage Publications. Retrieved on December 15 2006, from <http://www.sagepub.co.uk/booksProdDesc.nav?prodId=Book227351>
- Littlewood, A. (2003) 'Cyberporn and moral panic: an evaluation of press reactions to pornography on the internet', *Library and Information Research*, 27(86), 8–18.
- McKenzie, S. (2000). *Child Safety on the Internet: An Analysis of Victorian Schools and Households using the Routine Activity Approach*. A thesis submitted to the University of Melbourne, February, 2000. Retrieved on December 15 2006, from <http://www.criminology.unimelb.edu.au/research/internet/childsafety/index.html>
- Mann, David and Sutton, Mike, (1999). NetCrime. More Change in the Organisation of Thieving, *British Journal of Criminology*, vol. 38, no. 2, Spring 1998.
- Thomas, D. and Loader, B. (2000) 'Introduction – cyber crime: law enforcement, security and surveillance in the information age', in: D. Thomas and B. Loader (Eds.), *Cyber crime: Law Enforcement, Security and Surveillance in the Information Age*, London: Routledge.
- Yar, M. (2005) The Novelty of 'Cyber crime': An Assessment in Light of Routine Activity Theory *European Journal of Criminology*, Volume 2 (4): 407–427:

The discipline of criminology has evolved in three phases, beginning in the 18th century. Although crime and criminals have been around for as long as societies have existed, the systematic study of these phenomena did not begin until the late 1700s. Prior to that time, most explanations of crime equated it with sin—the violation of a sacred obligation. When scholars first distinguished crime from sin, they made possible explanations of criminal behavior that were not theological (religious). In Western Europe, the United States, and Canada, criminologists expanded their professional associations and published an increasing number of journals. A number of universities developed graduate programs in criminology.