International Journal of Cyber Criminology
Vol 1 Issue 2 July 2007

EDITORIAL

Establishing a Theory of Cyber Crimes

K. Jaishankar

I have developed a theory called ***'Space Transition Theory'*** in order to explain the causation of crimes in the cyberspace. I felt the need for a separate theory of cyber crimes because the general theoretical explanations were found to be inadequate as an overall explanation for the phenomenon of cyber crimes (Jaishankar 2008). I have published this theory as a chapter in a book titled *"Crimes of the Internet"* edited by Frank Schmalleger & Michael Pittaro, published by Prentice Hall (2008: 283-301). "*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 cyberspace (Jaishankar 2008). Space transition involves the movement of persons from one space to another (e.g., from physical space to cyberspace and vice versa). Space transition theory argues that, people behave differently when they move from one space to another.

The postulates of the theory are:

1. *Persons, with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position.*
2. *Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cyber crime*
3. *Criminal behavior of offenders in cyberspace is likely to be imported to Physical space which, in physical space may be exported to cyberspace as well.*
4. *Intermittent ventures of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape.*
5. *(a) Strangers are likely to unite together in cyberspace to commit crime in the physical space.*
   (b) Associates of physical space are likely to unite to commit crime in cyberspace.
6. *Persons from closed society are more likely to commit crimes in cyberspace than persons from open society.*
7. *The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cyber crimes.*

Since criminology has started viewing the emergence of cyberspace as a new locus of criminal activity, a new theory is needed to explain why cyber crime occurs. The space transition theory presented above provides an explanation for the criminal behavior in the cyberspace. There is a need to test the *Space Transition Theory* to see if it explains cyber criminal activity (Jaishankar 2008).

The second issue of the journal has a varied range of articles written by emerging and established experts in the field of Cyber Criminology. The first article by Russell Smith is about how advances in information and communications technologies (ICT) have created a range of new crime problems but it has also facilitated prevention, detection, investigation, prosecution and punishment of crime. This paper identifies the principal areas of human rights concern which the digital age has created. The paper concludes with the ways by which the infringement of human rights in the digital age could be prevented. They suggest that rigorous evaluative research needs to be conducted once new technologies have been introduced in order to monitor their potential for denigration of human rights and infringements of international and national laws.

The second article by Michael L. Pittaro is an introduction to online harassment and intimidation which is termed as cyber stalking. In this paper he has discussed about how internet has facilitated criminal activities. He states that cyber stalking is an extension of traditional stalking but is not as predictable as the traditional stalking. The author gives some cases of cyber stalking and how things have become very easy for the criminal to harass his victim. The crime of cyber stalking is linked with mental abnormality and gives a clear picture why such incidents happen. Author states ways to avoid being a victim in such cases which are suggested by the law enforcement officials. Author concludes saying that though the problem is in its infancy stage, it's growing rapidly.

The third article, entitled, 'Are We Protecting Our Youth Online?' is written by Catherine D. Marcum. This paper starts with a brief introduction of origin of internet and the protective measures taken by the Government to prevent online victimization of youth. This paper discusses the use of filtering and blocking software as one of the major proactive measures. Success of proactive prevention programs and other types of online safety measures is limited. The first and most imperative step to protection of children online is educating them on why it is important to avoid certain behaviors and places on the Internet. Through the use of protective tools and other informative measures, it is a must to make internet a safe place for the youth and young, as it was intended.

The fourth paper by Michael Bachmann from University of Central Florida talks about the Recording Industry Association of America (RIAA) which is a lawsuit that was set up to prevent the illegal sharing of music files. Despite these legal efforts, results show that the majority of music downloaders show little awareness of wrongdoing and in turn the popularity of P2P networks has been steadily increasing. Paper provides the data, results and conclusions of various studies on this topic that have been carried out. Apart from that the implications for the music and video industry as well as future research are discussed. Future studies should examine the successfulness of the efforts employed by the MPAA and the role that increasingly popular legal download alternatives have for the pirating of copyright-protected material.

In Article five, Kasun Jayawardena and Roderic Broadhurst talk about the online exploitation of children. This paper provides an initial exploration of the role Web 2.0 network technology may play in providing access to underage victims who may be vulnerable to on-line sexual predators. They have presented their research on the topic with proper methodology adopted for the study, the data and conclusions. They conclude that it is essential to empower children to police the Internet and to recognize their rapid absorption of the changes released by Web 2.0 and the relentless privatization and commercialization that is now increasingly apparent.

There are two book reviews in this issue. The book entitled, *"CYBERCRIME – The Reality of the Threat"* written by Nigel Phair, is reviewed by Nicholas Chantler of Queensland University of Technology. He opines that this book is an easy read introductory text on Cyber crime, which is based on the authors work experience as a Federal Agent in Australian High Tech Crime Centre in Canberra and as a member of the Australian Federal Police. He mentions about the possibility of fading of trust on the e-commerce by the internet users who get tapped in the web of online crimes. He also briefly mentions the profile of cyber crime criminals. Geographical overviews of the cyber crime elements are also presented. The book addresses the cyber crime activities under the broad headings like Unwanted Software, Identity Crime, Phishing, Critical Infrastructure Protection, Intellectual Property, Communications, Terrorism and Enforcement - recommendations and perspectives relating to the law enforcement response.

The book review of James Bowers, Jr., is about the book entitled, *"Cybercrime: How to avoid becoming a victim"* by H. Thomas Milhorn. He feels that this is a book that educates its readers about the different types of cyber crimes and ways in which internet users can protect them from becoming victims. Special emphasis in this book is given to defining what constitutes each type of crime, poignant examples of actual crimes, and finally, useful tips for protecting yourself from each type of crime. The chapters cover a broad range of topics. Auction fraud, job scams, charity scams, child pornography, copyright violation, cramming and slamming, credit card fraud, credit repair scams, cyber bullying, and cyber extortion Also, immigration fraud, investment fraud, laptop theft, loan scams, lottery scams, Nigerian fraud, overpayment scams, predatory scams, predatory behavior, pyramid schemes, prostitution, sales fraud, and spam, are dealt. Lastly, travel scam, viruses, and hoaxes are discussed. In a nutshell, the book covers all the types of cyber crime and ways to avoid being a victim.

Acknowledgements

I am grateful to Mili M. Krishnan, the editorial assistant, for assisting me in proof reading the articles, a voluntary work she undertook, in spite of her busy regular work. I am happy and proud to mark that, International Journal of Cyber Criminology (IJCC) is now abstracted/indexed in Directory of Open Access Journals, EBSCO, Intute, J V Barry Library Australian Institute of Criminology, Australian Institute of Police Management Library, University of Portsmouth Library, J-gate, and Index of Information Systems Journals. I thank all those Managers/Librarians involving in abstracting/indexing IJCC. I thank all the Editorial Advisory board members who sincerely reviewed the articles and for contributing to the continuing quality of articles. My earnest thanks are due to Dr. Robert G. Morris, University of Texas at Dallas, who recently joined the International Editorial Advisory Board, for significantly assisting me in reviewing articles. My special thanks go to the outside reviewer of this issue, Dr. Prapon of Bangkok Police Department. My heartfelt thanks go to the authors for their continuous support in making IJCC as one of the leading journals of the dynamic field of Criminology.

Reference

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