Book Review of Crime-Online

Debarati Halder
National Law School of India University, Bangalore, India


In the present internet era the three glaring problems that have outsmarted the cyber security professionals, lawmakers, law practitioners, police and the common individuals are hacking and hacking related activities, infringement of privacy; involvement and use of women and children in the sex trade through the internet and copyright violations. Laws are being made on the basis of researches that are being presented for national interests. But in reality, more researches are needed for creating ‘awareness camps’ among individual practitioners, cyber victim counsellors and especially common people who Google for anything and everything. This has practically motivated many academicians to go for a minute research of the issues pertaining to cyber crimes. While authored books present excellent opportunities for readers to know the viewpoints of the author(s) in a broader sense, edited volumes are conglomerations of numerous views which provide an array of ideas and Crime-online is one scintillating book in this regard.

This book is an edited version comprising the thoughts and ideologies of nine lead authors along with several other co-authors on various forms of crimes that happen on-line and their possible remedies. Reading this book was a pleasant experience for me especially because of the carefully edited chapters, tables and figures. The book mainly covers five types of crimes that happen on-line; i.e. hacking, infringement of privacy, issues of child sexual as well as non-sexual offences in the internet, online sex trade and negative effects of social engineering through cyber theft. All the nine chapters are authored by experienced professionals who have carefully presented the problems and perspectives along with the supporting data. Some these chapters also discuss the scope and usability of the present laws towards preventing the problems and restitution of justice to the victims. The book also discusses about several criminological theories in the light of patterns of crimes that have been discussed here.

The book opens with the chapter of Editor Holt’s introduction on the book and online crime. He has emphasized on the Wall’s (2007) frame work of four major types of cyber crimes, namely, cyber trespass, cyber deception/theft, cyber porn and obscenity and cyber violence. Chapter 3 by Taylor, throws light on hacking and how it aids to wicked people’s criminal motives. Chapter 5 by Rogers and Spellar discusses about child pornography in the light of recent legal developments in the US. This chapter elaborates
the issue with the help of case studies, which will help readers to understand the problem easily. Chapter 7 by Catherine Marcum discusses about cyber bullying and cyber stalking and the evaluation of laws to address these problems. This chapter also emphasizes on the free speech issues. This is very interesting as both bullying and execution of stalking may involve free speech issues. Chapter 8 by Britz deals with cyber terrorism and mechanism of it. For any researcher who aspires to work on cyber terrorism, this chapter promises to be immensely helpful. The book ends with the chapter (9) authored by Holt, Bossler and Fitzgerald and it deals with analysis of state and local law enforcement perceptions of computer crime. The most interesting part of this chapter is the data related to the policing of the cyberspace by the law enforcement officers. Even though I have come across many scholarly write ups on policing the cyber space and problems related to them, I have rarely seen such brilliant application of empirical analysis of the problem.

Even though each chapter presents unique point of views, I found chapters 2, 4 and 6 extremely interesting. While chapter 2 by Cassie Wade et.al highlights the motives of hacking along with other issues related to hacking and the mentality of the hacker, chapter 4 by Huang and Brockman throws light on the issue of cyber theft that is done in a very camouflaged fashion, namely through online communication and social engineering. The authors have brilliantly highlighted the psychological pressure on the victims to reveal their personal data to the perpetrators. Chapter 6 by Cunningham and Kendall on the other hand covers online sex trade from a distinctive point of view. The minute research on the characteristics and practices of the online prostitutes deserves particular mention.

The editor has considerably given ample freedom to all the authors to air their views and perspectives in different fashions and from different angles. This makes the book very useful not only for the undergraduate students of criminology, but also for law and other social science streams. Considering the price of it, this book should find a place in every college/university student’s library. The book is a must read for the police personnel, lawyers and cyber crime data and security professionals, as this will help them to understand traditional as well new trends of online crimes. The book will be immensely useful for researchers as well. Any researcher of digital communication, law and criminology would love to know about the recent trends of crimes that are happening online, the past and present scenario and the future impacts of the same. This book presents all of them. Further, the editor, himself an accomplished academician, maintains a uniform formatting of the pages right from the editorial chapter till the last index page. The book proves to be an excellent compilation of brilliant research works by 19 dedicated authors and I believe that this book will adorn almost all of the libraries of major universities and colleges that deal with criminology and law.