International Journal of Cyber Criminology
Vol 4 Issue 1&2 January - July 2010 / July - December 2010

Book Review of Cybercrime: An Introduction to an Emerging Phenomenon

Calli Price[1]
Truman State University, U.S.A.

Cybercrime: An Introduction to an Emerging Phenomenon, George Higgins, 2010, McGraw-Hill Publishing, New York, NY, 192 pages, U.S. $52.83 (Paperback), ISBN-10: 0073401552

Cybercrime is a relatively new concern for law enforcement officials. As the number of computer owners connected to the internet increases, so too does the opportunity for cyber crime. To fully understand the development of cyber crime one must study the language and culture of the internet as well as the pathways that connect users from around the world. This book explains how the internet works and describes the types of crime generally committed via a computer and the internet. The author deems this knowledge essential to combat the recent surge in internet-related offences.

This book begins with an introduction of emerging technological advancements and computer usage and relates these to how cyber crime threatens the security of internet users. The stated objective of this book is to give readers a basic understanding of this issue. *Cybercrime* is a small book, comprising just 187 pages. Though it is full of technical information, its writing style is clear and concise and will not confuse readers with long and unnecessary passages or terminology. Visual aides are occasionally offered but are not generally needed since material is understandable and can be read quickly.

Cybercrime is made up of eight chapters that outline the types and frequencies of various computer crimes currently being committed and the impact that these crimes will likely have in the future. Chapter titles include *Cyber-pornography* (3), *Identity Theft* (4), *Hackers* (6), and *Criminal Justice and Cyberspace* (7). Each chapter begins with an explanation of its title and how it applies to the book's overall objective. Also included are reviews of additional studies conducted by other cyber criminologists. For example, in Chapter 3, there are two papers presented on cyber-pornography. The first "examines the influence of technology on the distribution and psychological implications of pornography" while the second "examines the theoretical rationale of why individuals use pornography over the Internet" (pg. 40). All references are cited at the end of each chapter and are followed by discussion questions.

The chapter on *Identity Theft* (4) contains valuable insight into how information is illegally acquired and misused. Subheadings include "*Guarding against Identity Theft*" and "*Information Confidentiality*." A diagram appears within this chapter titled "*A Contextual*

[1] Student, Justice Systems Department, Truman State University, Kirksville, Missouri, United States of America. Email: clp3367@truman.edu

Framework for Combating Identity Theft" that provides a contextual framework about how information flows on a global basis (pg. 77). This diagram allows readers to visualize the process of identity theft and how it can be addressed.

Chapter 6, *Hackers*, contains information about those who seek to access computers and computer networks without authorization. Hacking is described as an act "imbued with innovation, style, and technical virtuosity" (pg. 130). Furthermore, this chapter places hacking in its proper historical context, tracing it to the advent of computer networking and the growing popularity of the internet. Without this knowledge, readers would be unable to fully understand how hacking has developed into a transnational problem. Examination of this subject is intended to help readers understand how important it is to be cautious with sensitive information. Furthermore, data-bases maintained by corporations and government agencies are in need of security measures to ensure that they are not breached.

While each chapter is important to the reader's understanding of internet-based crime, Chapter 8, *Future Issues*, certainly peaked my interest. It is within this chapter that the importance of privacy is discussed as a major concern for the future. Privacy in this context concerns the confidentiality of personal information. "Because of the internet's still embryonic state of existence, and its globally distributed nature, internet users have yet to organize a concerted effort to authoritatively declare a demand for the implementation of privacy protection mechanisms" (pg. 172). The author suggests that future efforts should be undertaken to safeguard information that is frequently stored on electronic media. These efforts may occur at the consumer and governmental levels.

Overall, this book is designed for both criminal justice officials and students that are looking for a quick introduction to the topic of computer crime. It takes basic subtopics of cyber crime and explains them in non-technical, layman's terms. It is small and easily understandable, so its readers will be able to use and reference it whenever needed. I recommend this book to those that want to increase their understanding of this interesting and often confusing topic. The author should be commended for making a broad and developing subject less perplexing. Any knowledge that can be acquired about computer-based crime, offender motivations and global offending patterns will prove useful to police and corrections officials as they are increasingly called upon to deal with this issue.