JISSec 3(1) 2007

Journal of Information System Security

www.jissec.org

Book Review

Digital Crime and Digital Terrorism

Robert W. Taylor, Tory J. Caeti,
D. Kall Loper, Eric J. Fritsch,
John Liederbach

Pearson/Prentice Hall, 2006, 397 pages
ISBN: 0-13-114137-6

Reviewed by: Michael Lapke

Introduction

The authors' intent in writing this book was to bridge the technical and knowledge gap that exists with many people in learning about computer/digital crime and digital terrorism. The reviewer's initial impression was that the authors not only achieved this goal but they did it in a clear yet thorough manner. This is a text that could be well utilized in an introductory computer crime course (whether the course is oriented towards a criminal justice (CJ) student or an information systems (IS) student). The book would also serve quite well as a reference guide for a CJ or IS practitioner.

The content of the book is thorough enough to give a reader a firm starting point in virtually any component of digital crime. The book does not go deeply into any of the specific technical aspects, either computer related or legal. For example, chapter six discusses viruses and malicious code. The chapter provides a good overview of the types of viruses, the differences between different viruses, the differences between viruses and worms/Trojan horses, etc. The broad overview provided in the chapter should be very helpful for a reader to get a baseline understanding of this type of digital crime. The chapter does not however linger in the technical details. A reader, for example, will not acquire the skills to write the code for creating a virus by reading this chapter. Nor would a reader learn any specific state or federal laws or how specific crimes are prosecuted.

The remainder of this review is divided into five sections. Four of the five sections discuss the four sections of the book. These discussions are critical in nature and judge the quality of each respective section. The first of these sections deals with "The Etiology of Digital Crime and Digital Terrorism." The second analyzes "Digital Crime - Types, Nature, and Extent." The third examines "Controlling Digital Crime: Legislation, Law Enforcement, and Investigation." The fourth investigates "The Future of Digital Crime and Digital Terrorism: Prevention and Trends." The final section of this review provides an overall judgment of the book.

Section I: The Etiology of Digital Crime and Digital Terrorism (Research Paper)

This section of the book is divided into four chapters: Introduction, Digital Terrorism, Criminology of Computer Crime, and Digital Criminals and Hackers. The term "etiology" refers to the assignment of a cause, an origin, or a reason for something. This section does just that: provides a probable cause for the existence of digital crime and digital terrorism. The first chapter does an adequate job of giving a broad overview and introduction to the content of the book. It covers new threats in the information age, the purpose of the book, definitions of digital crime and digital terrorism, and provides a taxonomy of different types of computer crime. As stated, the chapter does an adequate job in introducing the material. The one complaint is that it is written a little dryly. The authors do outline the chapter (and the remainder of the book for that matter) but do not provide any justification for the structure. Understanding why the chapter and book is organized the way it is would go a long way in helping the reader position him or herself to best understand the material.

The second, third, and fourth chapters are the most captivating of the entire book. For a reader with little experience in digital terrorism, the theories behind digital crime, and the culture of hackers, these chapters will make for a fascinating read. While it is limited in depth, the second chapter, which discusses digital terrorism, is a very good primer. It clearly defines the concepts, describes the types of attacks, and gives a brief overview of the two major players in digital terrorism: Al Qaeda and China. Chapter three gives a comprehensive overview of four categories of theories behind the criminology of computer crime: psychological, social structure, social process, and political. This chapter is the most fundamental to the etiology of digital crime, from an academic point of view.

The fourth and final chapter in the section, dealing with hacker culture, is the most enjoyable and intriguing portion of the book. The general populace tends to think of this subculture when they hear about computer security. The image of a grungy "evil genius" in the basement causing havoc around the world piques the public's interest. The authors do an incredible job painting a detailed and accurate picture of this subculture and pointing out that they're actually not the primary threat to the security of IS.

Section II: Digital Crime - Types, Nature, and Extent (Research Paper)

Though it still maintains a readable and interesting content, the book becomes slightly disjointed at this point. There is no transition from the first section to the second. Instead, the fourth chapter simply ends and the fifth chapter begins. Never-the-less, the chapters contained in this section will be singularly reviewed. The section of the book is divided into four chapters: White Collar Crimes, Viruses and Malicious Code, Exploitation, Stalking, and Obscenity on the WWW, and Anarchy and Hate on the WWW.

As with the rest of the book, the fifth chapter does a good job giving a solid foundation in its content. The content, white collar crimes, is discussed in an easy to read and comprehensive manner. The chapter is divided into subsections discussing the taxonomy of white collar crime. These sections include embezzlement, corporate espionage, money laundering, identity theft, and internet fraud schemes. The same comments can be made of chapter 6, which covers viruses and malicious code. This chapter gives a solid foundation in an easy to read and comprehensive manner. Chapter 7, which covers exploitation, stalking and obscenity on the World Wide Web, is also complete. The reviewer's main critique of these three chapters is that there is a lack of justification or structure. Why did the authors pick white collar crimes as the first "type" of digital crime? Are viruses a "type" of digital crime or a "nature" of digital crime?

Chapter 8 covers anarchy and hate. While fascinating topics, the reviewer does not understand why these two constructs are grouped together, since they represent two different concepts. Another problem the reviewer had was that chapter 8 also is heavily focused on digital terrorism. Why is this area included under the "digital crime" arena of section II? Since the book itself makes the distinction between crime and terrorism, shouldn't the chapters within the book follow that same taxonomy? Furthermore, terrorism tends to span well beyond simple "hate" or "anarchism." It seems an awkward title for a chapter that focuses on digital terrorism.

Section III: Controlling Digital Crime: Legislation, Law Enforcement, and Investigation (Research Paper)

Fortunately, the book regains a good amount of cohesion that was absent in section two when it moves to the third section. The area being covered is clear and the chapters which make up the meat of the area make logical sense. There is still a missing transition between sections two and three but this is not as apparent as the previous section change. This section of the book is divided into four chapters: Digital Laws and Legislation, Law Enforcement Roles and Responses, The Investigation of Computer-Related Crime, and Digital Forensics.

Given that the reviewer is not versed in laws or legislation (whether they be digitally oriented or otherwise), chapter 9 proved to be insightful. It gives an easy to read but thorough discussion of federally based laws and legislation. As an IS security practitioner, the information provided was essential. Chapter 10, which discusses law enforcement roles, is also astute. The agencies involved in digital crime go far beyond what the reviewer thought he knew. Chapter 11 discusses the investigation of computer-related crime. The reviewer was aware of most of the procedures discussed but the clear and concise writing style was refreshing. The technical orientation of chapter 12, which focuses on forensic analysis, was a welcome oasis for the reviewer. The previous three chapters are full of pertinent information but the reviewer felt at home reading about drive imaging, storage systems, and file systems.

Section IV: The Future of Digital Crime and Digital Terrorism: Prevention and Trends

This section receives a mixed review from the reviewer. The section is divided into two chapters: (1) Information Security and Infrastructure Protection and (2) Digital Crime and Terrorism: A Forecast of Trends and Policy Implications. The first of these two chapters, which deals with infrastructure protection, does not address any future issues in terms of information security. The topics covered, which include risk analysis and security technologies, are mature topics that have been extensively covered in other texts. The last chapter, which covers digital terrorism, is a good read though. The concept of terrorist forecasting is a pertinent and interesting issue.

Conclusion

As stated in the introduction, this book is a very good read for either a student or a practitioner. It is technical enough for either of these types of readers to have a background in IS yet it is legally thorough enough for those with a CJ background. The primary detriment to the book is the lack of structure of the second section. This section lacks the coherency and flow of the first and third sections. Also related to this is the lack of transition between sections. It is customary for books that have chapters within sections to recap the major points of each section and justify why they decided to group the chapters within a given section. All in all though, this book is a definite recommended read for practitioners of CJ or IS security. The content is solid and presented in a palatable manner.