

Book Review

Cybercrime and Digital Forensics

Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar

Routledge, London & New York

ISBN: 978-0-367-36006-1 (hbk)

ISBN: 978-0-367-36007-8 (pbk)

ISBN: 978-0-429-34322-3 (ebk)

DOI: 10.4324/9780429343223

The rapid proliferation of digital technologies has fundamentally transformed the ways in which individuals interact with the world. Activities such as shopping, communication, and information sharing are now predominantly conducted in digital environments possibilities that were unimaginable just a few decades ago. However, this evolution in human behavior, driven by technological innovation, has also created unprecedented opportunities for crime and misuse. Over the past thirty years, the integration of technology into everyday life has not only enabled traditional street criminals to expand their activities but has also given rise to entirely new forms of cybercrime.

In this context, *Cybercrime and Digital Forensics* provides a comprehensive exploration of the wide spectrum of cybercrimes. The book examines how conventional crimes have adapted to technological environments, as well as how entirely new forms of deviant behavior have emerged. A distinctive feature of the text is its focus on online subcultures associated with various forms of crime and deviance. By analyzing the norms, values, and practices within these subcultures, the authors offer insights into how participation in such groups shapes behavior both online and offline, and influences attitudes toward criminality. Furthermore, the book addresses legal frameworks across different jurisdictions and outlines the roles of local, national, and international law enforcement agencies in combating cybercrime.

The opening chapter sets the stage by presenting a lucid and comprehensive overview of the key issues related to technology and cybercrime. It effectively introduces the reader to the complexities and challenges inherent in understanding cybercriminal behavior in a rapidly evolving digital landscape. Chapter 2, *Law Enforcement, Privacy, and Security in Dealing with Cybercrime*, provides an overview of the various entities involved in policing cybercrime. These include traditional local, state, and federal law enforcement agencies, as well as private organizations and industry bodies that actively work to mitigate cybercrime, often without formal legal mandates.

Chapters 3 through 6 focus on specific types of cyber offenses. Chapter 3, *Computer Hackers and Hacking*, offers an in depth exploration of hacking activities and their impact on individuals and organizations. Chapter 4, *Malware and Automated Computer Attacks*, examines the evolution and functioning of malicious software. Chapter 5, *Digital Piracy and Intellectual Property Theft*, discusses how the Internet facilitates the theft of intellectual property, including proprietary algorithms and design plans. Chapter 6, *Online Fraud*, addresses various forms of online fraud and financial theft, such as email scams targeting unsuspecting victims.

Chapters 7 and 8 delve into cyber-enabled sexual offenses. Chapter 7, *Pornography, Image-Based Sexual Abuse, and Prostitution*, explores a range of online sexual behaviors and examines how the Internet has reshaped traditional forms of prostitution, as well as the responses of the criminal justice

system. Chapter 8, *Child Sexual Exploitation Material Offences*, focuses on crimes involving children, including the production, distribution, and consumption of child sexual exploitation materials (CSAM), as well as other forms of abuse.

The interpersonal dimensions of cybercrime are examined in Chapter 9, *Cyberbullying, Online Harassment, and Cyberstalking*, which highlights the growing prevalence of online harassment and its consequences. Chapter 10, *Online Extremism and Cyberterror*, analyzes how digital platforms are used to disseminate hate speech and extremist ideologies globally. Chapter 11, *Cyberwarfare and Information Operations Online*, extends this discussion to the geopolitical level, exploring how nation-states and individuals engage in cyberwarfare and coordinated information operations.

Chapter 12, *Illicit Market Operations Online*, investigates the functioning of illegal online marketplaces, including those operating on the Dark Web, where a wide range of illicit goods such as drugs, identity documents, and cybercrime tools are traded.

Chapter 13, *Cybercrime and Criminological Theories*, provides a theoretical perspective by examining whether traditional criminological theories are sufficient to explain cybercrime or whether new theoretical frameworks are required. This chapter offers a critical analysis of existing theories in light of emerging digital behaviors.

The final set of chapters focuses on digital forensics. Chapter 14, *Evolution of Digital Forensics*, outlines the development of forensic practices in digital contexts. Chapter 15, *Acquisition and Examination of Forensic Evidence*, discusses the tools and techniques used in evidence collection, data recovery, and analysis. Chapter 16, *Legal Challenges in Digital Forensic Investigations*, addresses issues related to the admissibility of digital evidence in court and the legal standards governing forensic investigations.

The concluding chapter, Chapter 17, *The Future of Cybercrime, Terror, and Policy*, reflects on the evolving nature of cyber threats and the challenges posed by the global and borderless character of digital technologies, which complicates efforts to regulate and control cybercrime effectively.

The book is further enriched by a well defined glossary and a comprehensive index, enhancing its usability as a reference work.

Overall, *Cybercrime and Digital Forensics* serves as a valuable resource for understanding contemporary cybersecurity issues. Its comprehensive coverage, analytical depth, and interdisciplinary approach make it a significant contribution to the study of cybercrime and digital forensics.

Hathairat Ketmaneechairat
Faculty of Information Technology, King Mongkut's University
of Technology North Bangkok, Bangkok, Thailand
hathairat.k@cit.kmutnb.ac.th