International Journal of Technoethics
Volume 11 • Issue 2 • July-December 2020

Book Review

Encyclopedia of Criminal Activities and the Deep Web (3 Volumes): Book Review

Reviewed by Arthur So, University of Ottawa, Canada
https://orcid.org/0000-0003-3479-6724

This book is reviewed by Arthur So, doctoral candidate, School of Electrical Engineering and Computer Science (EECS), University of Ottawa, Ottawa, Canada.

Edited by Mehdi Khosrow-Pour, the *Encyclopedia of Criminal Activities and the Deep Web* contains 79 chapters, divided into five sections over the three volumes. Mehdi Khosrow-Pour received his Doctorate in Business Administration from Nova Southeastern University (Florida, USA). Then Mehdi Khosrow-Pour taught undergraduate and graduate information system courses at the Pennsylvania State University – Harrisburg for almost 20 years. He is now the Executive Editor at IGI Global (www.igi-global.com). He also serves as Executive Director of the Information Resources Management Association (IRMA) (www.irma-international.org) and Executive Director of the World Forgotten Children Foundation (www.worldforgottenchildren.org). According to IGI Global (www.igi-global.com/affiliate/mehdi-khosrow-pourdba/346853), he is also author and editor of over 100 books in information technology management and 50 articles published in various conference proceedings and scholarly journals.

This collection includes perspectives from information technologists to illustrate the shortcomings of technologies and the exploitations of tools used in electronic frauds committed on the World Wide Web (WWW). The *Encyclopedia* also contains information on resources that are not searchable by a conventional search engine, which is referred to as the *Deep* and *Dark Web,* or they are called the *Invisible Webs*. The three volumes contain multidisciplinary research and expert insights provided by 130 leading researchers from 30 countries, including the United States, the United Kingdom, Australia, New Zealand, Germany, Finland, South Korea, Malaysia, and more. The entries are presented in an encyclopedia-style, providing diverse methodologies of monitoring and regulating the use of online tools in both open and invisible web. Hence, this work provides a comprehensive understanding of the use of online tools and existing software and hardware vulnerabilities used for cyberattacks. Consequently, it is essential reading for policymakers, lawmakers, cyberusers, and other stakeholders wishing to develop strategies for the prediction and prevention of online criminal activity.

Cyberusers evolve from using informational Web 1.0 to transactional Web 2.0 websites, resulting from the rapid growth of the development of e-Business and e-Commerce, and changing brick-and-

mortar businesses to online operations (Aghaei, Nematbakhsh, & Farsani, 2012). The *Encyclopedia of Criminal Activities and the Deep Web* describes major approaches facilitating business transactions, e-commerce, banking, and social media communications that change the lifestyle of a society. Furthermore, the *Encyclopedia* examines how these developments have also resulted in a significant rise in online criminal activities, like identity theft and cyberattacks, which are conducted over the *Deep Web*.

The preface, written by the editor Khosrow-Pours, provides the overall content of an encyclopedia-like structure of the book. Khosrow-Pours describes how cybercrimes are committed over different types of webpages (surface, deep, and dark web), and the enablers are technologies and social media networks according to the contents in the three volumes. The book contains valuable discussions of the ways that cybercriminals exploit the vulnerabilities of technology and human behaviour. The harmful outcomes cause a threat to organizations, businesses, governments, and other cyberusers, as illustrated by the articles in the book. The diverse and comprehensive coverage of this book contributes awareness and understanding of criminal activities and the Deep Web. The following book review describes some of the essential contents in a selected or group of chapters of similar research that readers might find them useful and informative in this cyber world.

The first volume (Chapters 1 – 15) establishes the foundation of the subsequent research by defining and identifying various types of cybercrimes that affect types of organizations and persons. Readers may need to read Chapter 1 (Thangamuthu, Rathee, Palanimuthu, & Balusamy) in detail to understand how cyberattacks are conducted and which steps are recommended to prevent cybercrimes. Additionally, the following discussions show some of the thrilling chapters in this volume. Some of the chapters cover particularly exciting topics. For example, Chapter 3 (Hoanca & Mock) describes the use of Artificial intelligence's capabilities for cyberattacks and clearly demonstrates the issues that security professionals should be aware of regarding the involvement of AI used in various cybercrimes. AI has resurgence its importance since its founding in 1956 at Dartmouth University due to the recent increase in computing processing power.

Chapter 8 (Elangoven) effectively illustrates the difference between the three types of web services (p. 129). The Surface Web is identified as having regular web pages representing 4 to 6% of the entire web pages; they are indexed in search engines, such as Google, Yahoo, etc. In contrast, the Deep Web represents approximately 90% of the web pages, which are not indexed in search engines; they include items such as medical records, government documents, and financial records (p. 129). The third web service is the Dark Web, which contains 6% of the web pages, and includes actionable information, drug trafficking, and political protests (p. 129). This chapter raised the alarm that most stakeholders are only aware of the Surface Web and not the Deep Web or the Dark Web. The following chapter, Chapter 9 (Herschel), examines the impacts of Dark Web activities on society. This chapter includes a discussion of legislation, including " the European Union's General Data Protection Regulation [GDPR] and the California Consumer Privacy Act" (p. 140). These rules govern how organizations must conform to the privacy of personal data collected online, and the author of this chapter uses the ethical theory to address the ethical issues of the Dark Web.

The first section of the second volume (Chapters 16 - 31) provides a thorough discussion of regulatory policies and solutions on cyberwarfare, cybersecurity, and spyware. A few chapters in this volume also provide analyses of cyber espionage, cyber-attacks, or cyberwarfare over computer networks in the 21st century. The authors of Chapter 20 (Singh & Ramdeo) and Chapter 21 (Awofeso) effectively discuss the management of whistleblowers and illustrate the whistleblower practice, respectively, through the use of various case studies focused on uncovering criminal activity in the health sector. Then, hacktivism and major hacking activities are discussed in detail in Chapter 22 (McMurtry & Stewart). The authors also compare the US Computer Fraud and Abuse Act of 1986 (CFAA) with similar laws in Korea, Germany, and China. From Chapters 25 to 31, the authors (Tiwari;

Wesley; Anglim; Rehman; Rehman; Tan et al.; Zaidenberg) respectively examine the different Internet regulations in various countries and explore how the Deep Web bypasses censorship with the use of virtual private networks (VPNs). For example, the challenge in implementing cybersecurity to protect cyberspace is discussed in Chapter 26 (Wesley) and Chapter 27 (Anglim). Still, the focus is mainly on the Deep Web in the context of the USA. Chapters 28 (Rehman), Chapter 29 (Rehman), and Chapter 30 (Tan et al.), the authors respectively discuss cybercrimes and cyber laws in the international context. All chapters in this section provide essential insights into the topics and engage closely with case studies to demonstrate the real-world applications of the issues.

The second section of the second volume (Chapters 32 - 48) contains a useful discussion of a few cases of drug and human trafficking and sexual exploitation of children. The authors of Chapters 32 (Kaur), 33 (Kejriwal) 34 (Whitney, Hultgren, Jennex, Elkins, & Frost) and 35 (Tan et al.) discuss drug trafficking and human smuggling, respectively. The authors show "various crimes such as identity theft, forgeries, child pornography, sex and human trafficking, terrorism and drug trafficking among others get efficiently planned and executed over a special and small part of the Internet, called the Dark Web" (Chapter 32, Kaur, p. 473). Anonymous web pages are used along with other technologies, such as TOR (The Onion Router), encryption, and cryptocurrencies. Sexual exploitation of children is discussed in Chapters 36 (Wallace), 37 (Crowell et al.) and 38 (Domfeld), reviewing mostly "child pornography, and more harmonization is required on both international and regional levels" (p. 575). The remaining Chapters 39 to 48 focus on hate crimes against women and hate speech, dark sites with social networking sites, cyberbullying and cyberstalking conducted on web pages and technological tools. The articles cover mostly US incidents and a few international cases. These articles correctly present those cybercrimes as having no boundary and assert that more future research on the elimination of such practices using the Dark Web may be needed, especially in the legal system.

The first section of volume 3 (Chapters 49 - 64) contains detailed discussions of financial fraud, identity theft, and social manipulation through social media networks. The authors of Chapters 49 to 54 discuss the threat and prevention of privacy disclosure over the Internet. They also highlight the challenges of safeguarding privacy when operating on the environment of the Internet of Things. Those articles that contribute details of personal information are not adequately protected in the Dark Web. I agree with the author in Chapter 54 (Marmo) in the identification of the cybercrimes conducted on commonly used cyber activities, like social networks and email. While the information provided was significant, the authors of this section did not discuss the need for changes to international laws because of the globalization characteristic of the Internet. The authors of Chapters 55 to 61 effectively illustrate different methods in identity theft via email spam, phishing, social media, and social engineering. Those articles provide a full guide for the types of frequent cyber attacks. The authors of Chapter 62 (Parthasarathi & Kaushal), Chapter 63 (Chea), and Chapter 64 (Broni, Boateng, & Owusu) review various financial frauds and the challenges and insights in managing e-Wallet and Bitcoin. Fraudulent in bitcoins and ransomware is a particularly complex area that the above articles simplify or explain in a clear way. In the second section of volume 3 (Chapters 65 to 79), the authors discuss security tools and solutions deployed in cyber defence and the social understanding of threats. The authors of this section provide innovative solutions, including human-based methods, to mitigate cyber risk and cybercrime activities on the worldwide web. This section also highlights the fast-growing technology causing societal problems and provide a full involvement of human behaviour.

While the *Encyclopedia* covered a wide array of topics, I think it would have been appropriate for Khosrow-Pour to include another section concerning infrastructures such as electricity grids and atomic plants. Because cyber criminals could compromise data produced from those automated operations and could cause disaster in society, including a discussion of these potential issues, would have helped to demonstrate the necessity of protecting these environments. Most of the readers believe technologies usually trigger cyberattacks on computing systems and not realize that automated power grids are prone to attacks too. Still, the second section of Volume 3 provides some more in-depth

analyses of human behaviour and ethics discussion of individual responsibility in Volume 1 while using the Internet.

Furthermore, this text made the critical point that the Surface Web is the tip of the iceberg in comparison to the Deep and Dark Web. There are many articles in this book exploring the invisible part of the web, but there should be more research articles on exposing the Deep and Dark Web. Improvement in exploring the Dark Web could be assisted by proper identification of encryption methods and the capability of avoiding anonymity. This approach would expose the Deep Web to ordinary cyberusers.

The *Encyclopedia of Criminal Activities and the Deep Web* contains plentiful examples of articles illustrating technical terminologies and definitions, types of cyberattacks, various cyberlaws, and potential solutions. Their findings led them to confirm that the Deep Web is causing more cyber vulnerabilities and personal information disclosure. However, since then, *blockchain* adoption in protecting data and transactions has become a "new kid in the block," This book should include the discussion of such an innovative digital transactional structure in eCommerce, securing future financial transactions in cloud computing with bitcoin.

Nevertheless, the main objective of this book is to highlight the editors' concerns about the existence of the Deep and Dark Web and the awareness of cybercriminals using these invisible webs to prey on cyberusers. The articles in this book have successfully illustrated the deficiencies of technologies and how cybercriminals exploit the vulnerabilities. The book has presented in an encyclopedia-like structure so that readers can review the cybercrimes systematically conducted on the invisible webs and the human responsibility in using the Internet. I strongly recommend this book to cyberusers, policymakers, lawmakers, and technology developers.

REFERENCES

Aghaei, S., Nematbakhsh, M. A., & Farsani, H. K. (2012). Evolution Of The World Wide Web: From Web 1.0 to Web 4.0. *International Journal of Web & Semantic Technology*, *3*(1), 1–10. doi:10.5121/ijwest.2012.3101

Khosrow-Pour, D. B. A. (Ed.). (2020). *Encyclopedia of Criminal Activities and the Deep Web* (Vols. 1–3). IGI Global. doi:10.4018/978-1-5225-9715-5

Arthur So is a PhD student at the University of Ottawa in the E-Business Technologies program, which is a multiple disciplinary endeavour between the Telfer School of Management, the School of Information Technology and Engineering, and the Faculty of Communication. Arthur has a Bachelor of Applied Science in Cybernetics and Computer Science from Reading University, UK; a Master in E-Business Technologies and a Master in Education, both from the University of Ottawa. He has worked in four different Departments of the Canadian federal and Quebec government and in the University of Ottawa, in technical areas including information technology security, mapping applications and network implementation. Arthur's research aims to acquire a more complete understanding of technoethics. The research will illustrate what happens when technology advances without any consideration for ethics and standards, as though technology, ethics and standards were unrelated elements. Arthur's major research attempts to achieve a better understanding of cyberbullying, as a subset of technoethics.