1.

Record Nr.	UNINA9910830147403321
Titolo	Cybercrime during the SARS-Cov-2 pandemic (2019-2022) : evolutions, adaptations, consequences / / edited by Daniel Ventre, Hugo Loiseau
Pubbl/distr/stampa	London, England : , : ISTE Ltd and John Wiley & Sons, Inc., , [2023] ©2023
ISBN	1-394-22634-9 1-394-22632-2
Descrizione fisica	1 online resource (256 pages)
Disciplina	345.730268
Soggetti	Computer crimes Computer viruses Criminal jurisdiction
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover -- Title Page -- Copyright Page -- Contents -- Introduction -- Chapter 1. The Evolution of Cybercrime During the Covid-19 Crisis -- 1.1. Introduction -- 1.2. Observing the evolution of cybercrime -- 1.2.1. Leveraging annual data: the case of India -- 1.2.2. Leveraging monthly data -- 1.2.3. Leveraging weekly data: the case of China -- 1.3. Has the global geography of cyberattacks changed? -- 1.4. Conclusion -- 1.5. Appendix -- 1.5.1. Cybercrime tools: malware -- 1.5.2. CVSS as indicators of vulnerability levels -- 1.5.3. Heterogeneity and complexity of cybercrime typologies -- 1.5.4. Attitude of companies toward cyber risks: the case of the United Kingdom -- 1.6. References -- Chapter 2. The SARS-CoV-2 Pandemic Crisis and the Evolution of Cybercrime in the United States and Canada -- 2.1. Introduction -- 2.2. The impacts of the SARS-CoV-2 pandemic -- 2.3. Cybercrime and SARS-CoV-2 -- 2.3.1. Targets and victims -- 2.3.2. Malicious actors -- 2.3.3. Cyberspace: a propitious environment for cybercrime -- 2.4. The evolution of cybercrime in North America during the pandemic -- 2.4.1. The United States -- 2.4.2. Canada -- 2.5. Discussion -- 2.6. Conclusion -- 2.7. Acknowledgments -- 2.8.

References -- Chapter 3. Online Radicalization as Cybercrime: American Militancy During Covid-19 -- 3.1. Introduction -- 3.2. A new typology of cybercrime -- 3.3. Internet connectivity and violent militancy -- 3.4. The pre-pandemic domestic threat landscape -- 3.5. The domestic threat landscape of the pandemic -- 3.6. Pandemic accelerationism -- 3.7. From virtual to real-life criminality -- 3.8. Online radicalization during Covid-19 -- 3.9. A new methodological paradigm for online radicalization? -- 3.10. Conclusion: meta-radicalization as cybercrime -- 3.11. References.

Chapter 4. Cybercrime in Brazil After the Covid-19 Global Crisis: An Assessment of the Policies Concerning International Cooperation for Investigations and Prosecutions -- 4.1. Introduction: Brazilian cybercrime and the Covid crisis impact -- 4.2. Cybercrime in the literature and the Brazilian case -- 4.3. A theoretical model for international cooperation -- 4.4. The evolution of cybercrime in Brazil -- 4.5. The evolution of the Brazilian legal system concerning cybercrime and its connection to the international regime -- 4.6. Managing international cooperation without having the best tools -- 4.7. Difficulties with cooperation: joints, mortises, and notches -- 4.8. Conclusion: what to expect from the future? -- 4.9. References -- 4.10. Appendix: List of interviews and questions -- Chapter 5. Has Covid-19 Changed Fear and Victimization of Online Identity Theft in Portugal? -- 5.1. Introduction -- 5.2. The impact of the Covid-19 pandemic on cybercrime -- 5.3. Evolution of cybercrime in Portugal -- 5.4. Online identity theft (OIT) -- 5.4.1. Definition and modus operandi -- 5.4.2. RAT applied to cyberspace -- 5.4.3. Individual variables and OIT victimization -- 5.5. Fear of (online) crime -- 5.5.1. Determinants of fear of (online) crime -- 5.6. The present study -- 5.6.1. Measures -- 5.6.2. Results -- 5.6.3. Variables associated with online victimization and fear of identity theft -- 5.7. Conclusion -- 5.8. References -- Chapter 6. A South African Perspective on Cybercrime During the Pandemic -- 6.1. Introduction -- 6.1.1. Background to South Africa and the pandemic -- 6.1.2. Methodology -- 6.2. International rankings -- 6.3. Cybercrime and related legislation -- 6.4. Cybersecurity incidents -- 6.4.1. Ransomware -- 6.4.2. Scams and fraud -- 6.4.3. System intrusions and data breaches -- 6.4.4. Disinformation and malicious communications -- 6.4.5. Other.

6.5. Discussion -- 6.6. Conclusion -- 6.7. References -- List of Authors -- Index -- EULA.