1. Record Nr. UNINA9910558483803321

Titolo	Cyber Security : Critical Infrastructure Protection / / edited by Martti Lehto, Pekka Neittaanmäki
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	3-030-91293-0
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (487 pages)
Collana	Computational Methods in Applied Sciences, , 2543-0203 ; ; 56
Disciplina	364.168 005.8
Soggetti	Data protection Computer crimes Cooperating objects (Computer systems) Data and Information Security Cybercrime Cyber-Physical Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Part I: Digital society. Chapter 1: Cyber-attacks Against Critical Infrastructure -- Chapter 2: Key Elements of On-line Cyber Security Exercise and Survey of Learning During the On-line Cyber Security Exercise -- Chapter 3: Cyber Law and Regulation -- Chapter 4: Understanding and Gaining Human Resilience Against Negative Effects of Digitalization -- Chapter 5: Users' Psychopathologies: Impact on Cybercrime Vulnerabilities and Cybersecurity Behavior -- Chapter 6: Process Ontology Approach to Military Influence Operations -- Part II: Critical infrastructure protection. Chapter 7: Future Smart Societies' Infrastructures and Services in the Cyber Environments -- Chapter 8: Cyber Security in Healthcare Systems -- Chapter 9: Cyber Security of an Electric Power System in Critical Infrastructure -- Chapter 10: Maritime Cybersecurity: Meeting Threats to Globalization's Great Conveyor.
Sommario/riassunto	This book focus on critical infrastructure protection. The chapters present detailed analysis of the issues and challenges in cyberspace and provide novel solutions in various aspects. The first part of the

book focus on digital society, addressing critical infrastructure and different forms of the digitalization, strategic focus on cyber security, legal aspects on cyber security, citizen in digital society, and cyber security training. The second part focus on the critical infrastructure protection in different areas of the critical infrastructure. The chapters cover the cybersecurity situation awareness, aviation and air traffic control, cyber security in smart societies and cities, cyber security in smart buildings, maritime cyber security, cyber security in energy systems, and cyber security in healthcare. The third part presents the impact of new technologies upon cyber capability building as well as new challenges brought about by new technologies. These new technologies are among others are quantum technology, firmware and wireless technologies, malware analysis, virtualization.