

1. Record Nr.	UNISA996465447703316
Titolo	Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity [[electronic resource] /] / edited by Hamid Jahankhani, Stefan Kendzierskyj, Nishan Chelvachandran, Jaime Ibarra
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-35746-5
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (viii, 450 pages) : illustrations
Collana	Advanced Sciences and Technologies for Security Applications, , 1613-5113
Disciplina	005.8
Soggetti	Artificial intelligence Big data Computer security System safety Artificial Intelligence Big Data Privacy Security Science and Technology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Foreword -- Part 1: Cyber Defence & Critical National Infrastructure (CNI) -- Critical National Infrastructure, C4ISR and Cyber Weapons in the Digital Age -- The Malicious Use of AI-based Deepfake technology as the New Threat to Psychological Security and Political Stability -- Considerations for the Governance of AI and Government Legislative Frameworks -- Part 2: Augmented Humanity & Digital Society -- Augmented humanity: Data, Privacy and Security -- Consumer Awareness on Security and Privacy Threat of Medical Devices -- Biohacking Capabilities & Threat/ Attack Vectors -- Digital Twins for Precision Healthcare -- 5G Cybersecurity Vulnerabilities with IoT and Smart Societies -- Part 3: Technology of Cyber Attacks -- Blockchain, TTP Attacks and Harmonious Relationship with AI -- Protecting Privacy and Security Using Tor and Blockchain and De-anonymization Risks --

Experimental Analyses in Search of Effective Mitigation for Login Cross-Site Request Forgery -- Attack Vectors and Advanced Persistent Threats -- Artificial Intelligence in Protecting Smart Building's Cloud Service Infrastructure from Cyberattacks -- Part 4: Smart Societies and Data Exploitation -- Smart Distributed Ledger Technologies in Industry 4.0: Challenges and Opportunities in Supply Chain Management -- Combating Domestic Abuse inflicted in smart societies -- Deep Convolutional Neural Networks for Forensic Age Estimation: a Review -- Secure Implementation of E-governance: a Case Study about Estonia -- Insider Threat.

---

Sommario/riassunto

This publication highlights the fast-moving technological advancement and infiltration of Artificial Intelligence into society. Concepts of evolution of society through interconnectivity are explored, together with how the fusion of human and technological interaction leading to Augmented Humanity is fast becoming more than just an endemic phase, but a cultural phase shift to digital societies. It aims to balance both the positive progressive outlooks such developments bring with potential issues that may stem from innovation of this kind, such as the invasive procedures of bio hacking or ethical connotations concerning the usage of digital twins. This publication will also give the reader a good level of understanding on fundamental cyber defence principles, interactions with Critical National Infrastructure (CNI) and the Command, Control, Communications and Intelligence (C3I) decision-making framework. A detailed view of the cyber-attack landscape will be garnered; touching on the tactics, techniques and procedures used, red and blue teaming initiatives, cyber resilience and the protection of larger scale systems. The integration of AI, smart societies, the human-centric approach and Augmented Humanity is discernible in the exponential growth, collection and use of [big] data; concepts woven throughout the diversity of topics covered in this publication; which also discusses the privacy and transparency of data ownership, and the potential dangers of exploitation through social media. As humans are become ever more interconnected, with the prolificacy of smart wearable devices and wearable body area networks, the availability of and abundance of user data and metadata derived from individuals has grown exponentially. The notion of data ownership, privacy and situational awareness are now at the forefront in this new age.

---