1. Record Nr. UNINA9910476756203321

Autore	Soldatos John
Titolo	Cyber-physical threat intelligence for critical infrastructures security : a guide to integrated cyber-physical protection of modern critical infrastructures / / John Soldatos
Pubbl/distr/stampa	Hanover, Massachusetts : , : Now Publishers, , [2020] ©2020
Descrizione fisica	1 online resource (xliii, 456 pages) : illustrations
Disciplina	005.8
Soggetti	Computer networks - Security measures Cyber intelligence (Computer security)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Preface -- Part I: Securing Critical Infrastructures of the Financial Sector -- Security Challenges for the Critical Infrastructures of the Financial Sector -- A Reference Architecture for Securing Infrastructures in the Finance Sector -- FINSTIX: A Security Knowledge Base for the Finance Sector -- Artificial Intelligence Gateway for Cyber-Physical Security in Critical Infrastructure and Finance -- Information Sharing and Stakeholders' Collaboration for Stronger Security in Financial Sector Supply Chains: A Blockchain Approach -- Automated Assistance to the Security Assessment of APIs for Financial Services -- Adaptive and Intelligent Data Collection for Security of Critical Financial Infrastructures and Services -- Part II: Securing Critical Infrastructures of the Health Sector -- Security Challenges for the Critical Infrastructures of the Healthcare Sector -- Security Systems in the Healthcare Sector -- Integrated Cyber-Physical Security Approach for Healthcare Sector -- Vulnerability and incident propagation in cyber-physical systems -- Innovative Toolkit to Assess and Mitigate Cyber Threats in the Healthcare Sector -- Part III: Securing Critical Infrastructures of the Energy Sector -- Security Challenges for the Critical Infrastructures of the Energy Sector -- Securing CEI by-designSecuring CEI by-innovation -- Part IV: Securing Critical Infrastructures of the Communications Sector -- Security and Resilience

Challenges for the Critical Infrastructures of the Communications Sector -- Resilience enhancement and risk control Platform for Communication Infrastructure Operators -- Managed Security on 5G communication networks: the Software Defined Security paradigm -- Part V: Sector Agnostic Issues in Critical Infrastructures Protection -- Detection of innovative low-rate denial of service attacks against critical infrastructures -- Resilience analysis and quantification for Critical Infrastructures -- CISIApro Critical Infrastructures Modelling technique for an effective Decision Making Support -- Modern innovative detectors of physical threats for Critical Infrastructures -- The Ethical Aspects of Critical Infrastructure Protection.

Sommario/riassunto

Modern critical infrastructures comprise of many interconnected cyber and physical assets, and as such are large scale cyber-physical systems. Hence, the conventional approach of securing these infrastructures by addressing cyber security and physical security separately is no longer effective. Rather more integrated approaches that address the security of cyber and physical assets at the same time are required. This book presents integrated (i.e. cyber and physical) security approaches and technologies for the critical infrastructures that underpin our societies. Specifically, it introduces advanced techniques for threat detection, risk assessment and security information sharing, based on leading edge technologies like machine learning, security knowledge modelling, IoT security and distributed ledger infrastructures. Likewise, it presets how established security technologies like Security Information and Event Management (SIEM), pen-testing, vulnerability assessment and security data analytics can be used in the context of integrated Critical Infrastructure Protection.The novel methods and techniques of the book are exemplified in case studies involving critical infrastructures in four industrial sectors, namely finance, healthcare, energy and communications. The peculiarities of critical infrastructure protection in each one of these sectors is discussed and addressed based on sector-specific solutions. The advent of the fourth industrial revolution (Industry 4.0) is expected to increase the cyber-physical nature of critical infrastructures as well as their interconnection in the scope of sectorial and cross-sector value chains. Therefore, the demand for solutions that foster the interplay between cyber and physical security, and enable Cyber-Physical Threat Intelligence is likely to explode. In this book, we have shed light on the structure of such integrated security systems, as well as on the technologies that will underpin their operation. We hope that Security and Critical Infrastructure Protection stakeholders will find the book useful when planning their future security strategies.