

1. Record Nr.	UNINA9910522596803321
Autore	Soldatos John
Titolo	Cyber-Physical Threat Intelligence for Critical Infrastructures Security : Securing Critical Infrastructures in Air Transport, Water, Gas, Healthcare, Finance and Industry // John Soldatos, Isabel Praca, Aleksandar Jovanovic
Pubbl/distr/stampa	Norwell, Massachusetts : , : Now Publishers, , 2021
Descrizione fisica	1 online resource (626 pages)
Disciplina	005.8
Soggetti	Cyber intelligence (Computer security)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Part I "Securing Critical Infrastructures of Sensitive Industrial Plants and Sites": *Chapter 1 "InfraStress approach on risk modelling of cascading events with live data for decision support". *Chapter 2 "Cyber-physical adversarial attacks and countermeasures for deep learning vision systems on critical infrastructures".*Chapter 3 "Modelling of interdependencies among and InfraStress approach on risk modelling of cascading events with live data for decision support". *Chapter 4 "Data Visualisation for Situational Awareness in Industrial Critical Infrastructure: an InfraStress Case Study".*Chapter 5 "Critical Infrastructures, SIPS and Threat Intelligence: legal and ethical aspects of security research".Part II "Securing Critical Infrastructures in the Water Sector": *Chapter 6 "Cyber security importance in the water sector and the contribution of the STOP-IT project".*Chapter 7 "Cyber-Physical security for critical water infrastructures at strategic and tactical level". *Chapter 8 "Cyber-physical solutions for real-time detection at operational level". *Chapter 9 "Applying Machine Learning and Deep Learning algorithms for Anomaly Detection in Critical Water Infrastructures".Part III "Securing Critical Infrastructures for Air Transport": *Chapter 10 "Security Challenges for Critical Infrastructures in Air Transport".*Chapter 11 "Toolkit to enhance cyber-physical security of Critical Infrastructures in Air Transport".*Chapter 12 "Security ontologies as technological enabler for blended threat

detection and enhanced systems interoperability".Part IV "Securing Critical Infrastructures for Gas": *Chapter 13 "Conceptual Model and CONOPS for Secure and Resilient Gas CI".*Chapter 14 "High-Level Reference Architecture (HLRA) for Gas Infrastructures Protection". *Chapter 15 "The SecureGas Key Performance Indicators for resilient gas critical infrastructures". *Chapter 16 "Communication of Security-related Incident Information to the Authorities and the Population".Part V "Securing Critical Infrastructures of the Healthcare Sector": *Chapter 17 "Security monitoring for medical devices".*Chapter 18 "User Experience models for threat monitoring and security management in healthcare". *Chapter 19 "Attacking and defending healthcare building automation networks".*Chapter 20 "An Intuitive Distributed Cyber Situational Awareness Framework Within a Healthcare Environment".Part VI "Securing Critical Infrastructures in the Finance Sector": *Chapter 21 "The FINSEC Platform: End-to-End Data-Driven Cyber-Physical Threat Intelligence for Critical Infrastructures in Finance". *Chapter 22 "Anomaly detection for critical financial infrastructure protection".Part VII "Critical Infrastructure Protection and Smart Resilience": *Chapter 23 "Indicator-based assessment of resilience of critical infrastructures: From single indicators to comprehensive "smart" assessment".

Sommario/riassunto

Modern critical infrastructures can be considered as large scale Cyber Physical Systems (CPS). Therefore, when designing, implementing, and operating systems for Critical Infrastructure Protection (CIP), the boundaries between physical security and cybersecurity are blurred. Emerging systems for Critical Infrastructures Security and Protection must therefore consider integrated approaches that emphasize the interplay between cybersecurity and physical security techniques. Hence, there is a need for a new type of integrated security intelligence i.e., Cyber-Physical Threat Intelligence (CPTI). This book presents novel solutions for integrated Cyber-Physical Threat Intelligence for infrastructures in various sectors, such as Industrial Sites and Plants, Air Transport, Gas, Healthcare, and Finance. The solutions rely on novel methods and technologies, such as integrated modelling for cyber-physical systems, novel reliance indicators, and data driven approaches including BigData analytics and Artificial Intelligence (AI). Some of the presented approaches are sector agnostic i.e., applicable to different sectors with a fair customization effort. Nevertheless, the book presents also peculiar challenges of specific sectors and how they can be addressed. The presented solutions consider the European policy context for Security, Cyber security, and Critical Infrastructure protection, as laid out by the European Commission (EC) to support its Member States to protect and ensure the resilience of their critical infrastructures. Most of the co-authors and contributors are from European Research and Technology Organizations, as well as from European Critical Infrastructure Operators. Hence, the presented solutions respect the European approach to CIP, as reflected in the pillars of the European policy framework. The latter includes for example the Directive on security of network and information systems (NIS Directive), the Directive on protecting European Critical Infrastructures, the General Data Protection Regulation (GDPR), and the Cybersecurity Act Regulation. The sector specific solutions that are described in the book have been developed and validated in the scope of several European Commission (EC) co-funded projects on Critical Infrastructure Protection (CIP), which focus on the listed sectors. Overall, the book illustrates a rich set of systems, technologies, and applications that critical infrastructure operators could consult to shape their future strategies. It also provides a catalogue of CPTI case studies in different sectors, which could be useful for security consultants and

practitioners as well.
