1. Record Nr. UNINA9911015967703321

Autore	Linkov Igor
Titolo	Cyber Resilience: Applied Perspectives / / edited by Igor Linkov, Alexander Kott
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-90109-6
Edizione	[2nd ed. 2025.]
Descrizione fisica	1 online resource (410 pages)
Collana	Risk, Systems and Decisions, , 2626-6725
Altri autori (Persone)	KottAlexander
Disciplina	621
Soggetti	Security systems Data protection Computer crimes Security Science and Technology Data and Information Security Cybercrime
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Fundamental Concepts of Cyber Resilience: Introduction and Overview -- Foundations of Cyber Resilience: The Confluence of Game, Control, and Learning Theories -- Analysis of Cyber Dependencies for Assessment of Cyber Resilience -- Quantifying and Reducing System Non-Resilience: Methodology, Metrics, and Case Study -- Navigating Socio-Technical Influences upon Cyber Resilience Adoption -- Resilient Decision Making in Cyber Incident Response -- Rule-Making for Insider Threat Mitigation -- Resilience in the Cloud-to-Things Continuum -- Experimental Measurements of Cyber Resilience -- Cyber-Physical Dimensions of Resilience Planning in National Security and Defense -- Regional Critical Infrastructure: a Cyber-Physical Resilience Assessment Methodology -- Supply Chains of Computer and Electronics Hardware Vulnerable to Climate Change, Counterfeiting, and Other Disruptions -- Active Defense Techniques for Enhancing Cyber Resilience -- Economic Resilience to Cyber Threats.
Sommario/riassunto	Resilience is defined as the ability to recover from or easily adapt to shocks and stresses. Resilience, unlike the concept of security (which is often and incorrectly conflated with resilience) refers to the system's

ability to recover or regenerate its performance after an unexpected impact produces a degradation in its performance. A clear understanding of distinction between security, risk and resilience is important for developing appropriate management of cyber threats. This books draws expertise from academia, industry, and government to present insightful discussion of the fundamental concepts of cyber resilience, including the most current technical issues, relevant methods and procedures, and recent developments of the field. This book offers greater emphasis on applying the concepts and methods of cyber resilience to practical problems as compared to our previous book. The bulk of the material is presented in a logical, consistent, and continuous way that is easily accessible to non-specialists and will be of use as teaching material as well as source of emerging scholarship in the field.