1. Record Nr. UNISA996465351503316

Titolo	Adaptive Autonomous Secure Cyber Systems [[electronic resource] /] / edited by Sushil Jajodia, George Cybenko, V.S. Subrahmanian, Vipin Swarup, Cliff Wang, Michael Wellman
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-33432-5
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (X, 289 p. 68 illus., 59 illus. in color.)
Disciplina	005.8
Soggetti	Computer security Artificial intelligence Computer communication systems Systems and Data Security Artificial Intelligence Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	3.2 Formalizing Data Triage Operations.
Nota di contenuto	1. Reference Architecture of an Autonomous Agent for Cyber Defense of Complex Military Systems -- 2. Defending against Machine Learning based Inference Attacks via Adversarial Examples: Opportunities and Challenges -- 3. Exploring Adversarial Artificial Intelligence for Autonomous Adaptive Cyber Defense -- 4. Can Cyber Operations be Made Autonomous? An Answer from the Situational Awareness Viewpoint -- 5. A framework for studying autonomic computing models in cyber deception -- 6. Autonomous Security Mechanisms for High-Performance Computing Systems: Review and Analysis -- 7. Automated Cyber Risk Mitigation: Making Informed Cost-effective Decisions -- 8. Plan Interdiction Games -- 9. Game Theoretic Cyber Deception to Foil Adversarial Network Reconnaissance -- 10. Strategic Learning for Active, Adaptive, and Autonomous Cyber Defense -- 11. Online Learning Methods for Controlling Dynamic Cyber Deception Strategies -- 12. Phishing URL Detection with Lexical Features and Blacklisted Domains -- 13. An Empirical Study of Secret Security Patch

in Open Source Software.

Sommario/riassunto

This book explores fundamental scientific problems essential for autonomous cyber defense. Specific areas include: Game and control theory-based moving target defenses (MTDs) and adaptive cyber defenses (ACDs) for fully autonomous cyber operations; The extent to which autonomous cyber systems can be designed and operated in a framework that is significantly different from the human-based systems we now operate; On-line learning algorithms, including deep recurrent networks and reinforcement learning, for the kinds of situation awareness and decisions that autonomous cyber systems will require; Human understanding and control of highly distributed autonomous cyber defenses; Quantitative performance metrics for the above so that autonomous cyber defensive agents can reason about the situation and appropriate responses as well as allowing humans to assess and improve the autonomous system. This book establishes scientific foundations for adaptive autonomous cyber systems and ultimately brings about a more secure and reliable Internet. The recent advances in adaptive cyber defense (ACD) have developed a range of new ACD techniques and methodologies for reasoning in an adaptive environment. Autonomy in physical and cyber systems promises to revolutionize cyber operations. The ability of autonomous systems to execute at scales, scopes, and tempos exceeding those of humans and human-controlled systems will introduce entirely new types of cyber defense strategies and tactics, especially in highly contested physical and cyber environments. The development and automation of cyber strategies that are responsive to autonomous adversaries pose basic new technical challenges for cyber-security. This book targets cyber-security professionals and researchers (industry, governments, and military). Advanced-level students in computer science and information systems will also find this book useful as a secondary textbook.