1.	Record Nr.	UNINA9910728948603321
	Autore	Kott Alexander
	Titolo	Autonomous Intelligent Cyber Defense Agent (AICA) : A Comprehensive Guide / / edited by Alexander Kott
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2023
	ISBN	9783031292699 3031292693
	Edizione	[1st ed. 2023.]
	Descrizione fisica	1 online resource (468 pages)
	Collana	Advances in Information Security, , 2512-2193 ; ; 87
	Disciplina	355.45
	Soggetti	Artificial intelligence Computer networks - Security measures Data protection - Law and legislation Artificial Intelligence Mobile and Network Security Privacy
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Chapter. 1. Autonomous Intelligent Cyber-defense Agent: Introduction and Overview -- Chapter. 2. Alternative Architectural Approaches -- Chapter. 3. Perception of Environment -- Chapter. 4. Perception of Cyber Threats -- Chapter. 5. Situational Understanding and Diagnostics -- Chapter. 6. Learning about the Adversary -- Chapter. 7. Response Planning -- Chapter. 8. Recovery Planning -- Chapter. 9. Strategic Cyber Camouflage -- Chapter. 10. Adaptivity & Antifragility -- Chapter. 11. Negotiation and Collaboration -- Chapter. 12. Human Interactions -- Chapter. 13. Testing and Measurements -- Chapter. 14. Deployment and Operation -- Chapter. 15. Command in AICA-intensive Operations -- Chapter. 16. Risk Management -- Chapter. 17. Policy Issues -- Chapter. 18. Development Challenges -- Chapter. 19. Case Study A: A Prototype Autonomous Intelligent Cyber-defense Agent -- Chapter. 20. Case Study B: AI Agents for Tactical Edge -- Chapter. 21. Case Study C: the Sentinel Agents.
	Sommario/riassunto	This book offers a structured overview and a comprehensive guide to

the emerging field of Autonomous Intelligent Cyber Defense Agents (AICA). The book discusses the current technical issues in autonomous cyber defense and offers information on practical design approaches. The material is presented in a way that is accessible to non-specialists, with tutorial information provided in the initial chapters and as needed throughout the book. The reader is provided with clear and comprehensive background and reference material for each aspect of AICA. Today’s cyber defense tools are mostly watchers. They are not active doers. They do little to plan and execute responses to attacks, and they don’t plan and execute recovery activities. Response and recovery – core elements of cyber resilience – are left to human cyber analysts, incident responders and system administrators. This is about to change. The authors advocate this vision, provide detailed guide to how such a visioncan be realized in practice, and its current state of the art. This book also covers key topics relevant to the field, including functional requirements and alternative architectures of AICA, how it perceives and understands threats and the overall situation, how it plans and executes response and recovery, how it survives threats, and how human operators deploy and control AICA. Additionally, this book covers issues of testing, risk, and policy pertinent to AICA, and provides a roadmap towards future R&D in this field. This book targets researchers and advanced students in the field of cyber defense and resilience. Professionals working in this field as well as developers of practical products for cyber autonomy will also want to purchase this book.