1. Record Nr. UNISA996547953403316

Titolo	Cyber deception : techniques, strategies, and human aspects / / Tiffany Bao, Milind Tambe, Cliff Wang, editors
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2023] ©2023
ISBN	3-031-16613-2
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (252 pages)
Collana	Advances in information security ; ; Volume 89
Disciplina	005.8
Soggetti	Computer networks - Security measures Cyberspace - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	1. Diversifying Deception: Game Theoretic Models for Two-Sided and Layered Deception -- 2. Human-Subject Experiments on Risk-based Cyber Camouflage Games -- 3. Adaptive Cyberdefense with Deception: A Human-AI Cognitive Approach -- 4. Cognitive Modeling for Personalized, Adaptive Signaling for Cyber Deception -- 5. Deceptive Signaling: Understanding Human Behavior against Signaling algorithms -- 6. Optimizing Honey Traffic Using Game Theory and Adversarial Learning -- 7. Mee: Adaptive Honeyfile System for Insider Attacker Detection -- 8. HoneyPLC: A Next-Generation Honeypot for Industrial Control Systems -- 9. Using Amnesia to Detect Credential Database Breaches -- 10. Deceiving ML-Based Friend-or-Foe Identification for Executables.
Sommario/riassunto	This book introduces recent research results for cyber deception, a promising field for proactive cyber defense. The beauty and challenge of cyber deception is that it is an interdisciplinary research field requiring study from techniques and strategies to human aspects. This book covers a wide variety of cyber deception research, including game theory, artificial intelligence, cognitive science, and deception-related technology. Specifically, this book addresses three core elements regarding cyber deception: Understanding human’s cognitive behaviors in decoyed network scenarios Developing effective deceptive strategies based on human’s behaviors Designing deceptive techniques that

supports the enforcement of deceptive strategies The research introduced in this book identifies the scientific challenges, highlights the complexity and inspires the future research of cyber deception. Researchers working in cybersecurity and advanced-level computer science students focused on cybersecurity will find this book useful as a reference. This book also targets professionals working in cybersecurity. Chapter 'Using Amnesia to Detect Credential Database Breaches' and Chapter 'Deceiving ML-Based Friend-or-Foe Identification for Executables' are available open access under a Creative Commons Attribution 4.0 International License via link. springer.com.