

Contents

1	Cyber War Games: Strategic Jostling Among Traditional Adversaries	1
	Sanjay Goel and Yuan Hong	
2	Alternatives to Cyber Warfare: Deterrence and Assurance	15
	Robert J. Elder, Alexander H. Levis and Bahram Yousefi	
3	Identifying and Exploiting the Cyber High Ground for Botnets	37
	Patrick Sweeney and George Cybenko	
4	Attribution, Temptation, and Expectation: A Formal Framework for Defense-by-Deception in Cyberwarfare	57
	Ehab Al-Shaer and Mohammad Ashiqur Rahman	
5	Game-Theoretic Foundations for the Strategic Use of Honeypots in Network Security	81
	Christopher Kiekintveld, Viliam Lisý and Radek Píbil	
6	Cyber Counterdeception: How to Detect Denial & Deception (D&D)	103
	Kristin E. Heckman and Frank J. Stech	
7	Automated Adversary Profiling	141
	Samuel N. Hamilton	
8	Cyber Attribution: An Argumentation-Based Approach	151
	Paulo Shakarian, Gerardo I. Simari, Geoffrey Moores and Simon Parsons	
9	The Human Factor in Cybersecurity: Robust & Intelligent Defense	173
	Julie L. Marble, W. F. Lawless, Ranjeev Mittu, Joseph Coyne, Myriam Abramson and Ciara Sibley	

10	CyberWar Game: A Paradigm for Understanding New Challenges of Cyber War	207
	Noam Ben-Asher and Cleotilde Gonzalez	
11	Active Discovery of Hidden Profiles in Social Networks Using Malware	221
	Rami Puzis and Yuval Elovici	
12	A Survey of Community Detection Algorithms Based On Analysis-Intent	237
	Napoleon C. Paxton, Stephen Russell, Ira S. Moskowitz and Paul Hyden	
13	Understanding the Vulnerability Lifecycle for Risk Assessment and Defense Against Sophisticated Cyber Attacks	265
	Tudor Dumitraş	
14	Graph Mining for Cyber Security	287
	B. Aditya Prakash	
15	Programming Language Theoretic Security in the Real World: A Mirage or the Future?	307
	Andrew Ruef and Chris Rohlf	

Cyber Warfare

Building the Scientific Foundation

Jajodia, S.; Shakarian, P.; Subrahmanian, V.S.; Coyan, V.; Wang, C. (Eds.)

2015, XIII, 321 p. 83 illus., 49 illus. in color., Hardcover

ISBN: 978-3-319-14038-4