1. Record Nr. UNINA9910299662503321

Titolo	Intelligent Methods for Cyber Warfare [[electronic resource] /] / edited by Ronald R. Yager, Marek Z. Reformat, Naif Alajlan
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-08624-3
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XII, 278 p. 58 illus.)
Collana	Studies in Computational Intelligence, , 1860-949X ; ; 563
Disciplina	005.82
Soggetti	Computational intelligence Artificial intelligence Computational Intelligence Artificial Intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Malware and Machine Learning -- Soft Computing Based Epidemical Crisis Prediction -- An ACP-Based Approach to Intelligence and Security Informatics -- Microfiles as a Potential Source of Confidential Information Leakage -- Decision Support in Open Source Intelligence -- Information Fusion Process Design Issues for Hard and Soft Information: Developing an Initial Prototype -- Intrusion Detection with Type-2 Fuzzy Ontologies and Similarity Measures -- A multi-objective genetic algorithm based approach for effective intrusion detection using neural networks -- Cyber Insider Mission Detection for Situation Awareness -- A Game Theoretic Engine for Cyber Warfare -- Mission Impact Assessment for Cyber Warfare -- Uncertainty modeling: the Computational Economists' View on Cyberwarfare.
Sommario/riassunto	Cyberwarfare has become an important concern for governmental agencies as well businesses of various types. This timely volume, with contributions from some of the internationally recognized, leaders in the field, gives readers a glimpse of the new and emerging ways that Computational Intelligence and Machine Learning methods can be applied to address problems related to cyberwarfare. The book includes a number of chapters that can be conceptually divided into three topics: chapters describing different data analysis methodologies with

their applications to cyberwarfare, chapters presenting a number of intrusion detection approaches, and chapters dedicated to analysis of possible cyber attacks and their impact. The book provides the readers with a variety of methods and techniques, based on computational intelligence, which can be applied to the broad domain of cyberwarfare.