Preface

The cyberspace has an overwhelming influence on everyday activities of individuals and organizations. It has become a crucial part of society, industry, and government. It is used as a repository of different types of information, including critical ones, and as a means to oversee many activities and undertakings of social as well as industrial nature. Any type of malevolence directed on cyberspace creates disruptions affecting large numbers of people, organizations, and companies. Any minor attack on the Internet, as the most prominent part of cyberspace, can cause uncountable damage and loss of information, and has the ability to distress people's activities, and paralyze corporations and governments.

This vulnerability of the cyberspace can be used to intentionally confuse, disrupt, and even stop normal functions of societies and organizations. In the light of our increased dependence on the proper and sound operation of the cyberspace, mechanisms and systems, preventing any disruption and malicious actions on the Internet is of critical importance. In other words, safety and security of cyberspace has become essential.

By Cyberwarfare, we mean situations in which one entity, individual or organization, attacks another entity through cyberspace for the purpose, among other things, of stealing information, effecting the performance of its adversaries computer environment or sabotaging physical or information centric systems. With the pervasive use of computers and the Internet, organizations have become more and more vulnerable to cyber attacks.

The techniques emerging from areas of Computational Intelligence and Machine Learning are destined to find their way to cyberwarfare-related applications. The currently developed and mature techniques of fuzzy logic, artificial neural networks, evolutionary computing, prediction and classification, decision-making techniques, game theory, and also information fusion can be used to address a broad range of issues and challenges related to prevention, detection and impact analysis of different intrusions and attacks on cyber infrastructure.

This volume gives readers a glimpse, by all means far from being comprehensive, on new and emerging ways that Computational Intelligence and Machine Learning methods can be applied to issues 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 issues, chapters presenting a number of instruction detection approaches, and chapters dedicated to analysis of possible cyber attacks and their impact. The book starts with a number of chapters related the topic of data and information processing methods. Machine Learning, fuzziness, decision-making, and information fusion are examples of topics and methods targeted by the following chapters.

The first chapter entitled "Malware and Machine Learning" by Charles LeDoux and Arun Lakhotia provides an overview of Machine Learning techniques and their application to detect different forms of malware. The similarities between malware that contains inherent patterns and similarities due to code and code pattern reuse, and Machine Learning that operates by discovering inherent patterns and similarities create an opportunity to explore a synergetic effect created via combining these two fields. The authors provide an overview of machine learning methods and how they are being applied in malware analysis. They describe the major issues together with an elucidation of the malware problems that machine learning is best equipped to solve.

Recognizing fuzzy logic-based techniques are some of the most promising approaches for crisis management is stimulated by Dan E. Tamir, Naphtali D. Rishe, Mark Last, and Abraham Kandel in their chapter "Soft Computing Based Epidemical Crisis Prediction". They focus on epidemical crisis prediction as one of the most challenging examples of decision making under uncertain information. According to the authors, the key for improving epidemical crises prediction capabilities is the ability to use sound techniques for data collection, information processing, and decision making under uncertainty. They point out that complex fuzzy graphs can be used to formalize the techniques and methods used for the data mining. Additionally, they assert that the fuzzy-based approach enables handling events of low occurrence via low fuzzy membership/truth-values, and updating these values as information is accumulated or changed.

An approach called ACP—Artificial societies, Computational experiments, and Parallel execution—is described and used for security-related purposes in the chapter "An ACP-Based Approach to Intelligence and Security Informatics" authored by Fei-Yue Wang, Xiaochen Li, and Wenji Mao. The authors focus on behavioral modeling, analysis and prediction in the domain of security informatics. Especially, they look at group behavior prediction and present two methods of doing it. The first approach uses plan-based inference that takes into consideration agents' preferences. The second approach uses graph theory and incorporates a graph search algorithm to forecast complex group behavior. The results of experimental studies to demonstrate the effectiveness of the proposed methods are presented.

Attacks on open information sources are addressed in the chapter "Microfiles as a Potential Source of Confidential Information Leakage" by Oleg Chertov and Dan Tavrov. In particular, they look at microfiles as an important source of information in cyberwarfare. They illustrate, using real data, that ignoring issues that ensure

group anonymity can lead to leakage of confidential information. They show that it is possible to define fuzzy groups of respondents and obtain their distribution using appropriate fuzzy inference system. They discuss methods for protecting distributions of crisp as well as fuzzy groups of respondents.

The issues related to open source intelligence are addressed by Daniel Ortiz-Arroyo who authored the chapter "Decision Support in Open Source Intelligence". The decision support system presented here has been developed within the framework of the FP7 VIRTUOSO project. At the beginning, the author describes the overall scope and architecture of the VIRTUOSO platform. Further, he provides details of the main components of the constructed decision support system. These components employ computational intelligence techniques—soft-fusion and fuzzy logic—to integrate and visualize, together with other VIRTUOSO tools, diverse sources of information, and to provide access to the knowledge extracted from these sources. Some applications of this system in cyber-warfare are described.

The process of integration of data and information is addressed in "Information Fusion Process Design Issues for Hard and Soft Information: Developing an Initial Prototype" by James Llinas. The author provides a thorough description of challenges and requirements imposed on data and information fusion systems providing support for decision-making processes in the military/defense domains. In these domains, the nature of decision-making ranges from conventional military-like to socio-political—also characterized as "hard" and "soft" decisions. Because of this, the nature of information required for analysis is highly diversified. The heterogeneity of available information is indicated as an important factor driving the data and information fusion process design. Overall, the author offers perspectives on how those new requirements affect the design and development of data and information fusion systems.

An important aspect of instruction detection is addressed in the next three chapters. The first of them—"Intrusion Detection with Type-2 Fuzzy Ontologies and Similarity Measures" by Robin Wikstrom and Jozsef Mezei—targets an issue of embedding experts' knowledge in detecting constantly changing intrusion types. The authors propose a framework based on fuzzy ontology and similarity measures to incorporate experts' knowledge to the process of identification of these anomalies and handling imprecise information. Such a framework allows for identification of attacks that have never been experienced before. The authors present a fuzzy ontology developed based on the intrusion detection needs of a financial institution.

Another approach for instruction detection is proposed by Gulshan Kumar and Krishan Kumar. In the chapter "A Multi-objective Genetic Algorithm Based Approach for Effective Intrusion Detection Using Neural Networks", they propose a novel multiobjective genetic algorithm (MOGA) based approach for effective intrusion detection based on benchmark datasets. The approach generates a pool of non-inferior solutions—detection systems—that optimize trade-offs of multiple conflicting objectives, and creates an ensemble of these solutions to detect intrusions. The approach consists of three phases: (1) a MOGA based generation of

solutions leading to creation of a Pareto front of non-inferior individual solutions; (2) a further refinement of the obtained solutions via identification of a Pareto front of ensemble solutions; and (3) an aggregation method used for fusing individual predictions to determine outcome of the ensemble-based detection system. The authors used two benchmark datasets: KDD cup 1999, and ISCX 2012 to demonstrate and validate the performance of the proposed approach for intrusion detection.

The next chapter starts with a brief review of exiting works in the Machine Learning community that offers treatments to cyber insider detection. Following this, the authors of "Cyber Insider Mission Detection for Situation Awareness"—Haitao Du, Changzhou Wang, Tao Zhang, Shanchieh Jay Yang, Jai Choi, and Peng Liu—introduce their own method for early detection of a mission of system's insider. The method uses Hidden Markov Models to estimate insider's levels of activities. Fuzzy rules and Ordered Weighted Average are used to fuse multiple facets of information about an intruder. Experimental results based on simulated data show that the integrated approach detects the insider mission with high accuracy and in a timely manner, even in the presence of obfuscation techniques.

Research activities that address an important objective aiming at better understanding of cyberwarfare scenarios, as well as impacts that different attacks have on multiple aspects of systems are presented next. Here, we have three versatile and important contributions.

The first of them "A Game Theoretic Engine for Cyber warfare" is dedicated to the application of game-theoretic principles to the cyberwarfare domain. Allen Ott, Alex Moir, and John T. Rickard—the authors of the chapter—look at application of a game theory to investigate behavior of an attacker and defender. They use a well-known Themistocles engine that has been developed and used over the past decade in cyberwarfare analysis, for the modeling and analysis of cyberwarfare offensive and defensive tactics. It is shown that generated courses of actions (COAs) for both offensive and defensive cyberwarfare scenarios are consistent with the move choices made by independent experts who monitor the game. The authors indicate future extensions such as fuzzification of move scores using both type-1 and interval type-2 membership functions, as well as utilization of hierarchical linguistic weighted power means for the aggregation of COA scores. All this will enable to handle inherent imprecision associated with the costs/benefits of individual moves.

The impact of cyber threats on a military network subjected to attacks is addressed in the next chapter "Mission Impact Assessment for Cyber warfare". The authors—Jared Holsopple, Shanchieh Jay Yang, and Moises Sudit—estimate impact of such threats on operations of a military system during its mission. They propose application of a tree-based structure, called a Mission Tree, to model relationships between missions, tasks, and assets. These relationships are modeled using Order Weighted Aggregators (OWAs), which address a diverse set of relationship types. The Mission Tree is capable of providing a quantitative estimate of and impact by propagating the impact "up," from the leaves to the root, through the tree. An important aspect of the impact assessment process proposed

in the chapter is related to constant changes of missions or tasks performed by the system. The authors explore how scheduled or non-scheduled changes should affect the mission tree and influence the impact assessment process.

Economical consequences of attacks are subject of the next chapter by Suchitra Abel entitled "Uncertainty Modeling: The Computational Economists' View on Cyberwarfare". The author analyzes factors affecting the security of internet-based business. A casual model-based security system that focuses on core characteristics of contemporary internet-based businesses is presented. It extends traditional utility-based models with Bayesian causal networks. These networks represent relationships between variables, internal, and external, influencing business activities in normal and under attack conditions.

We hope that the readers will enjoy this book and that they will benefit from the useful and interesting methods and techniques conveyed by the authors in the broad domain of cyberwarfare.

New Rochelle, USA — Ronald R. Yager
Riyadh, Saudi Arabia — Naif Alajlan
Edmonton, Canada — Marek Z. Reformat

http://www.springer.com/978-3-319-08623-1

Intelligent Methods for Cyber Warfare
Yager, R.R.; Reformat, M.; Alajlan, N. (Eds.)
2015, XII, 278 p. 58 illus., Hardcover
ISBN: 978-3-319-08623-1