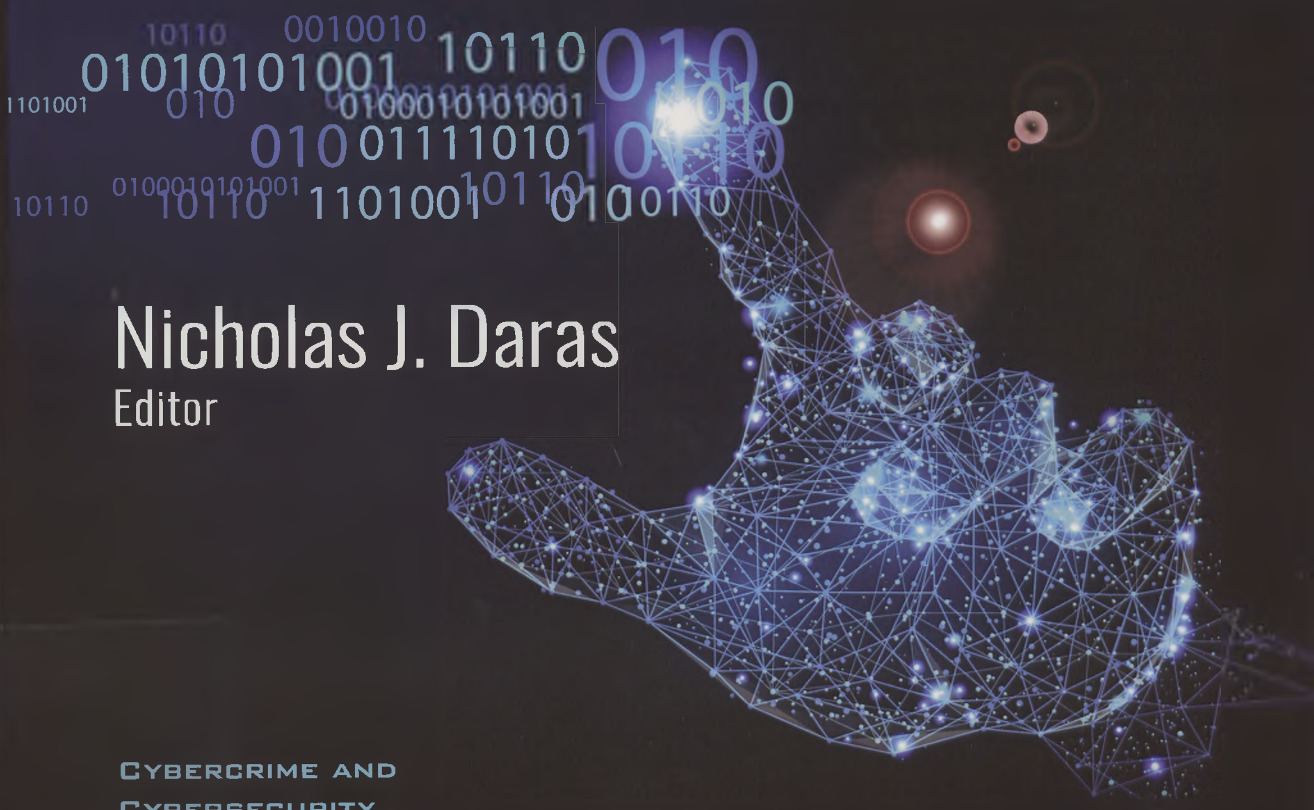
Cyber-Security and Information Warfare



Nicholas J. Daras
Editor

Cybercrime and
Cybersecurity
Research

NOVA

CYBERCRIME AND CYBERSECURITY RESEARCH

CYBER-SECURITY AND INFORMATION WARFARE

Cybercrime and Cybersecurity Research

Additional books and e-books in this series can be found
on Nova's website under the Series tab.

CYBERCRIME AND CYBERSECURITY RESEARCH

CYBER-SECURITY AND INFORMATION WARFARE

NICHOLAS J. DARAS
EDITOR

BIBLIOTEKA
Nr ewid. ....
Akademii Sztuki Wojennej

nova
science publishers
New York

Copyright © 2019 by Nova Science Publishers, Inc.

All rights reserved. No part of this book may be reproduced, stored in a retrieval system or transmitted in any form or by any means: electronic, electrostatic, magnetic, tape, mechanical photocopying, recording or otherwise without the written permission of the Publisher.

We have partnered with Copyright Clearance Center to make it easy for you to obtain permissions to reuse content from this publication. Simply navigate to this publication's page on Nova's website and locate the "Get Permission" button below the title description. This button is linked directly to the title's permission page on copyright.com. Alternatively, you can visit copyright.com and search by title, ISBN, or ISSN.

For further questions about using the service on copyright.com, please contact:
Copyright Clearance Center
Phone: +1-(978) 750-8400 Fax: +1-(978) 750-4470 E-mail: info@copyright.com.

NOTICE TO THE READER

The Publisher has taken reasonable care in the preparation of this book, but makes no expressed or implied warranty of any kind and assumes no responsibility for any errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of information contained in this book. The Publisher shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the readers' use of, or reliance upon, this material. Any parts of this book based on government reports are so indicated and copyright is claimed for those parts to the extent applicable to compilations of such works.

Independent verification should be sought for any data, advice or recommendations contained in this book. In addition, no responsibility is assumed by the publisher for any injury and/or damage to persons or property arising from any methods, products, instructions, ideas or otherwise contained in this publication.

This publication is designed to provide accurate and authoritative information with regard to the subject matter covered herein. It is sold with the clear understanding that the Publisher is not engaged in rendering legal or any other professional services. If legal or any other expert assistance is required, the services of a competent person should be sought. FROM A DECLARATION OF PARTICIPANTS JOINTLY ADOPTED BY A COMMITTEE OF THE AMERICAN BAR ASSOCIATION AND A COMMITTEE OF PUBLISHERS.

Additional color graphics may be available in the e-book version of this book.

Library of Congress Cataloging-in-Publication Data

ISBN: 978-1-53614-385-0

Published by Nova Science Publishers, Inc. † New York

CONTENTS

Preface ix

Chapter 1 SHERLINUX- A Tool Facilitating Linux Forensics 1
Antonios Andreatos

Chapter 2 Acoustic Scattering for a Piecewise Homogeneous Obstacle 25
Christodoulos E. Athanasiadis and Evangelia S. Athanasiadou

Chapter 3 Economic Implications of the Rise of Information Warfare, Cyber-War and Cyber-Security 39
Kyriaki Athanassouli

Chapter 4 Cyber Warfare: A Beyond the Basics Approach 57
Nikolaos Benias and Sozon A. Leventopoulos

Chapter 5 Real-Time Computational Intelligence Protection Framework against Advanced Persistent Threats 83
Konstantinos Demertzis and Lazaros Iliadis

Chapter 6 Computer Ethics and Institutions 109
Maria Dimarogona and Petros Stefaneas

Chapter 7 Notes on the Estimation of the Asymptotics of the Moments for the *m* Collector's Problem 129
Aristides V. Doumas

Chapter 8 The Use of Millimeter and Sub-Millimeter Wave Frequencies in Future Military Applications 137
M. Gargalakos, I. Karanasiou, R. Makri and N. K. Uzunoglu

Chapter 9 On the Mechanics of Nanocomposite Structures Using Multiscale Computational Techniques **159**
Stylianos K. Georgantzinos

Chapter 10 Operational Analysis and Crisis Management (OACM) Framework: The Paradigm of 2011 Military Intervention in Libya **175**
Dionysios Gerontogiannis

Chapter 11 Artificial Intelligence in Cyber Defense **193**
Georgios Karapilafis

Chapter 12 A Case Study Analysis of Attacks and Losses in the Supply Chain with the Use of GPS or GSM Jammers by the Attackers **201**
Panayiotis Laimos, Michalis Chronopoulos, Chrysanthi Laimou and Nikoleta Atanasova

Chapter 13 Dynamic Response of Protein Microtubules **211**
A. K. Lazopoulos

Chapter 14 Time Temperature Superposition Response of Carbon Fiber Reinforced Composite Plaques under Accelerated Aging Conditions **221**
Dionysios E. Mouzakis and Stefanos P. Zaoutsos

Chapter 15 Attacks against Information Systems in the E.U. Environment: Legal Texts and the Joint Cybercrime Action Taskforce (J-Cat) Model **237**
Anastasios Papathanasiou and Georgios Germanos

Chapter 16 The Military Applications of Printed Flexible Electronics **243**
Fotios Pelesis

Chapter 17 The Computational Simulation of Passive Synchronization Method for Frequency Hopping Systems **259**
K. A. Psilopanagiotis and P. E. Atlamazoglou

Chapter 18 Economics, Financial Warfare and Economic Espionage: From Total War to Modernity. An Analysis of Selected Case Studies **271**
Ioannis-Dionysios Salavrakos

Chapter 19 Ethics in Cyberspace: Cyber-Security **325**
Stamatia Sofiou

Chapter 20 Bivariate Copulas-Based Models for Communication Networks **337**
Ioannis S. Triantafyllou

Chapter 21 Redesigning the Flood Training Unit of the Hellenic Navy: Principles and Aspects of Human Centered Design **347**
G. V. Lykos, N. P. Ventikos, A. K. Rammos and V. G. Petropoulos

Chapter 22 An Automated Procedure for the Utilization of Hellenic Army's Empty Warehouses **361**
Theodoros Zikos, Dimitrios Zaires and Nikolaos V. Karadimas

Editor Contact Information **381**

Index **383**

Biblioteka Główna
Akademii Sztuki Wojennej
26644/III (CB)
03-026644-000-0

A variety of modern researc cyber-security techniques a gies are provided in this boo developments and support applications from engineering. This allows for the exploration of new approaches, useful practices and related problems for further investigation.

Distinguished researchers and scientists coming from different scientific origins present their research and views concerning cyber-security, information warfare and communications systems.

Graduate students, scientists and engineers interested in a broad spectrum of current theories, methods, and applications in interdisciplinary fields will find this book invaluable.

Topics covered include: Electronic crime and ethics in cyberspace, new technologies in security systems/systems interfaces, economic information warfare, digital security in the economy, human factor evaluation of military security systems, cyber warfare, military communications, operational analysis and information warfare, and engineering applications to security systems/detection theory.

nova
science publishers
www.novapublishers.com

ISBN 978-1-53614-385-0
9 781536 143850