

Advanced Sciences and Technologies for Security Applications

Series editor

Anthony J. Masys, Associate Professor, Director of Global Disaster Management, Humanitarian Assistance and Homeland Security, University of South Florida, Tampa, USA

Advisory Board

Gisela Bichler, California State University, San Bernardino, CA, USA

Thirimachos Bourlai, WVU - Statler College of Engineering and Mineral Resources, Morgantown, WV, USA

Chris Johnson, University of Glasgow, UK

Panagiotis Karampelas, Hellenic Air Force Academy, Attica, Greece

Christian Leuprecht, Royal Military College of Canada, Kingston, ON, Canada

Edward C. Morse, University of California, Berkeley, CA, USA

David Skillicorn, Queen's University, Kingston, ON, Canada

Yoshiki Yamagata, National Institute for Environmental Studies, Tsukuba, Japan

The series *Advanced Sciences and Technologies for Security Applications* comprises interdisciplinary research covering the theory, foundations and domain-specific topics pertaining to security. Publications within the series are peer-reviewed monographs and edited works in the areas of:

- biological and chemical threat recognition and detection (e.g., biosensors, aerosols, forensics)
- crisis and disaster management
- terrorism
- cyber security and secure information systems (e.g., encryption, optical and photonic systems)
- traditional and non-traditional security
- energy, food and resource security
- economic security and securitization (including associated infrastructures)
- transnational crime
- human security and health security
- social, political and psychological aspects of security
- recognition and identification (e.g., optical imaging, biometrics, authentication and verification)
- smart surveillance systems
- applications of theoretical frameworks and methodologies (e.g., grounded theory, complexity, network sciences, modelling and simulation)

Together, the high-quality contributions to this series provide a cross-disciplinary overview of forefront research endeavours aiming to make the world a safer place.

The editors encourage prospective authors to correspond with them in advance of submitting a manuscript. Submission of manuscripts should be made to the Editor-in-Chief or one of the Editors.

More information about this series at <http://www.springer.com/series/5540>

Dimitris Gritzalis • Marianthi Theocharidou
George Stergiopoulos
Editors

Critical Infrastructure Security and Resilience

Theories, Methods, Tools and Technologies

 Springer

Editors

Dimitris Gritzalis
Department of Informatics
Athens University of Economics
and Business
Athens, Greece

Marianthi Theocharidou
Directorate E. Space, Security and Migration
European Commission – Joint Research
Centre
Ispra, Italy

George Stergiopoulos
Department of Informatics
Athens University of Economics
and Business
Athens, Greece

ISSN 1613-5113 ISSN 2363-9466 (electronic)
Advanced Sciences and Technologies for Security Applications
ISBN 978-3-030-00023-3 ISBN 978-3-030-00024-0 (eBook)
<https://doi.org/10.1007/978-3-030-00024-0>

Library of Congress Control Number: 2018961423

© Springer Nature Switzerland AG 2019

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Part I Governance & Risk Management

Resilience Approach to Critical Information Infrastructures	3
Eric Luijff and Marieke Klaver	
Methodologies and Strategies for Critical Infrastructure Protection	17
Nikolaos Petrakos and Panayiotis Kotzanikolaou	
Risk Analysis for Critical Infrastructure Protection	35
Richard White	
Risk-Based Analysis of the Vulnerability of Urban Infrastructure to the Consequences of Climate Change	55
Erich Rome, Manfred Bogen, Daniel Lückerath, Oliver Ullrich, Rainer Worst, Eva Streberová, Margaux Dumonteil, Maddalen Mendizabal, Beñat Abajo, Efrén Feliu, Peter Bosch, Angela Connelly, and Jeremy Carter	

Part II Dependencies & Network Analysis

Identification of Vulnerabilities in Networked Systems	79
Luca Faramondi and Roberto Setola	
Game-Theoretic Decision Making for the Resilience of Interdependent Infrastructures Exposed to Disruptions	97
Yiping Fang and Enrico Zio	
Smallest Pseudo Target Set Identification and Related Problems Using the Implicative Interdependency Model	115
Arun Das, Chenyang Zhou, Joydeep Banerjee, Anisha Mazumder, and Arunabha Sen	
Leveraging Network Theory and Stress Tests to Assess Interdependencies in Critical Infrastructures	135
Luca Galbusera and Georgios Giannopoulos	

Part III Industrial & Automation Control Systems

Micro-Grid Control Security Analysis: Analysis of Current and Emerging Vulnerabilities	159
Peter Beaumont and Stephen Wolthusen	
Engineering Edge Security in Industrial Control Systems	185
Piroska Haller, Béla Genge, and Adrian-Vasile Duka	
Secure Interconnection of IT-OT Networks in Industry 4.0	201
Cristina Alcaraz	

Part IV Cybersecurity

Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin	221
Henry Mwiki, Tooska Dargahi, Ali Dehghantanha, and Kim-Kwang Raymond Choo	
Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management	245
Georgia Lykou, George Iakovakis, and Dimitris Gritzalis	
Open Source Intelligence for Energy Sector Cyberattacks	261
Anastasis Keliris, Charalambos Konstantinou, Marios Sazos, and Michail Maniatakos	
A Taxonomy of Side Channel Attacks on Critical Infrastructures and Relevant Systems	283
Nick Tsalis, Efstratios Vasilellis, Despina Mentzelioti, and Theodore Apostolopoulos	