

Advances in Information Security

Volume 84

Series editor

Sushil Jajodia, George Mason University, Fairfax, VA, USA

The purpose of the *Advances in Information Security* book series is to establish the state of the art and set the course for future research in information security. The scope of this series includes not only all aspects of computer, network security, and cryptography, but related areas, such as fault tolerance and software assurance. The series serves as a central source of reference for information security research and developments. The series aims to publish thorough and cohesive overviews on specific topics in Information Security, as well as works that are larger in scope than survey articles and that will contain more detailed background information. The series also provides a single point of coverage of advanced and timely topics and a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook.

More information about this series at <http://www.springer.com/series/5576>

Roberto Di Pietro • Simone Raponi
Maurantonio Caprolu • Stefano Cresci

New Dimensions of Information Warfare

 Springer

Roberto Di Pietro
Hamad Bin Khalifa University
College of Science & Engineering
Education City
Doha, Qatar

Simone Raponi
Hamad Bin Khalifa University
College of Science & Engineering
Education City
Doha, Qatar

Maurantonio Caprolu
Hamad Bin Khalifa University
College of Science & Engineering
Education City
Doha, Qatar

Stefano Cresci
National Research Council
Institute of Informatics and Telematics
Pisa, Italy

ISSN 1568-2633

ISSN 2512-2193 (electronic)

Advances in Information Security

ISBN 978-3-030-60617-6

ISBN 978-3-030-60618-3 (eBook)

<https://doi.org/10.1007/978-3-030-60618-3>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2021

This work is subject to copyright. All rights are solely and exclusively licensed 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, expressed 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

Foreword

It would be difficult to imagine our daily life, our production systems and, in general, our society without the technology solutions we are immersed in and surrounded by. However, technology, and in particular information technology, is a double-edged sword.

The capillary diffusion and reach of social networks enable us to communicate our ideas to the world, but they could easily be used to spread fake news; the adoption of digitized industrial control systems is rewarded with a boost in cost reduction, efficiency and performance, but those very same controls can also make the controlled systems much more fragile; the advent of novel digital financial instruments and tools, from high-frequency trading to cryptocurrencies, do multiply the possibility to trade and to access financial instruments, but they also pose a threat, for the policy makers, to the control of the financial leverage; technologies that have been developed for entertainment, such as drones, have expanded to a number of no-one-envisioned-before applications and jobs, but they also enabled the possibility of physical attacks through the very same media.

Technology has drastically reduced the distance between ideas and implementation, projects, and outcomes. This is just a logical consequence of what technology is: a magnifier of our capabilities. Nowadays, a 240-character piece of news, conveyed to hundreds of millions, could sink the NYSE or skyrocket the price of a share. An induced malicious glitch in a water-desalinization or oil-extraction pressure controller could induce the outage of critical infrastructure and spur, according to the allegedly attribution, geo-political tensions in vast regions of the world. Similarly, the use of a social network by billions of young people can slowly induce, by subtle AI algorithms, new life models and different values to new generations—potentially creating domestic turmoil of an unprecedented magnitude.

As a result, the technology transformed the society so in-depth and so quickly that almost all the essential functions and services of a Nation have been digitalized; this is why even the decision on the very same adoption of an apparently neutral

technology, such as the 5G, or which data can be exploited by a social network company, could lie with the Department of State as a national security matter rather than with a technical, bureaucratic desk. This means every nation needs to set appropriate cyber defenses in terms of sociological, legal, organizational, and technical issues to cope with the complexity and threats induced by the cited technology waves that could harm the very pillars of our democracies, putting at stake even the values of our new generations. While initially lagging behind these threats, States and Supranational Organizations have started to respond. For instance, at the EU level the Network and Information Security (NIS) directive and the “Cybersecurity act” are being implemented. In the USA, each government organization is involved on a daily basis to implement its own piece of a multidimensional Cybersecurity Strategy regularly revised by the White House to take both latest technology development and its social-economic implications into account. In Italy, the Parliament has recently passed a law: “National Security Perimeter for Cyber”, whose mission is twofold: (1) to create a more resilient Country by reinforcing security measures for essential functions and services of the State through a complex techno-legal organization and (2) to foster a strategic plan to achieve an intended degree of digital sovereignty.

As a consequence of the previous arguments, it is true more than ever that “Information (and the technology used to manage it) is power”. It is no surprise, therefore, that Information Warfare—roughly, the manipulation of information trusted by a target without the target’s awareness—is a topic that cannot be anymore restricted to the battlefield. The one who is able to control or influence information within a given ecosystem (ranging from your ring of friends to industry, finance, and politics, to cite a few) can exercise a form of control over that ecosystem.

The above scenarios and considerations do pave the way to a number of fundamental questions, such as: What are the novel boundaries of Information Warfare? What technologies are today critical to that respect? To which extent the very fabric of our society, economics and critical infrastructures can be affected by Information Warfare?

All the above-introduced questions do require urgent attention and, especially, a framework that sets the tone of the discussion, highlights the assets at stakes, and suggests the objectives to be achieved. That is why I found this book a gripping read. It introduces a novel vision on Information Warfare, addressing relevant dimensions of Information Warfare so far overlooked, puts them in context, highlights the main strategical and tactical assets, and provides the tools for an educated discussion on the topic. The cited key features, combined with the clear exposition, the pleasant style, the comprehensive references and the links to real-world cases, do make this book a reference for technologists, decision-makers, practitioners, academicians and insiders. But what is more, this book also provides food for thought for all the ones who are aware that information technology and its nemesis, Information Warfare, are playing a vital role in the evolution and shaping of our Society. A Society that is

in dire needs to elaborate a strategic reflection on the novel dimensions and threats posed by Information Warfare.

Deputy Director General
Department of Information for Security
Presidency of Ministry Council of Italy
Rome, Italy
August 27, 2020

Prof. Roberto Baldoni*

*Roberto Baldoni is currently on leave from the Sapienza University of Rome, where he is a full professor of computer science. As DIS Deputy DG, Baldoni chairs the Italian Cybersecurity Management Board (Nucleo Sicurezza Cibernetica—NSC), an inter-ministerial organization established at DIS via executive decree (DPCM 2/2017). NSC implements and oversees the prevention and management of nationwide cyber crises coordinating National CSIRT, Postal Police (Ministry of the Interior), the Inter-Force Cyber Command (Ministry of Defense) and the intelligence agencies. NSC is also responsible for national cybersecurity policy positions in international forums and for fostering cybersecurity cooperation between government, research and industry. Roberto Baldoni led the working group designing the Decree Law 105/2019 “National security perimeter for cyber”, and in 2020, he is acting, on behalf of the Inter-ministerial Committee for Security of the Italian Republic (CISR), as roll-out coordinator for the Legislative Decree 105/2019.

Contents

- 1 New Dimensions of Information Warfare 1**
 - 1.1 Organization 3
 - 1.1.1 Book Structure 3
 - 1.1.2 Infoboxes 3
- Part I Society**
- 2 Information Disorder 7**
 - 2.1 The New Social Ecosystem 10
 - 2.2 Scenario 1: Freedom of Information 13
 - 2.2.1 Threat: Disinformation Campaign 14
 - 2.2.2 Attacks 15
 - 2.3 Scenario 2: Democratic Election in a Country 23
 - 2.3.1 Threat: Interference in Political Election 24
 - 2.3.2 Attacks 25
 - 2.4 Countermeasures 33
 - 2.4.1 Low-Quality Information 34
 - 2.4.2 Malicious Actors 44
 - 2.5 Open Issues and Future Directions 61
 - 2.5.1 New Directions 62
- Part II Economy**
- 3 Cryptocurrencies 69**
 - 3.1 State-Sponsored Cryptocurrency 70
 - 3.2 Scenario 1: Trust in Maths 71
 - 3.2.1 Threat: Collapse of the Cryptocurrency Foundation 73
 - 3.2.2 Attacks and Countermeasures 74
 - 3.2.3 Open Issues 76
 - 3.3 Scenario 2: Trust in the Computational Power 78
 - 3.3.1 Threat: New Technologies 79
 - 3.3.2 Threat: Collusion Among Miners 82

3.3.3	Open Issues	86
3.4	Scenario 3: Infrastructure	87
3.4.1	Threat: Hijacking Network Infrastructure	88
3.4.2	Attacks and Countermeasures	90
3.4.3	Open Issues	93
3.5	Toward a State-Sponsored Cryptocurrency	93
3.5.1	Bitcoin Limitations	94
3.5.2	Develop a State-Sponsored Cryptocurrency	95
4	FinTech	99
4.1	Scenario 1: Stock Market Forecasts	104
4.1.1	Threat: Information-Based Manipulation	107
4.1.2	Threat: Trade-Based Manipulation	113
4.1.3	Threat: Algorithm-Based Manipulation	119
4.1.4	Other Countermeasures	130
4.2	Scenario 2: High-Frequency Trading	131
4.2.1	Threat: Technological Bias, Divide, and Monopoly	135
4.2.2	Attacks and Countermeasures	135
4.2.3	Open Issues and Future Directions	137
4.3	Scenario 3: Remote Stock Market	138
4.3.1	Threat: Attacks Against Availability	140
4.3.2	Threat: Work-from-Home Perils	144
4.3.3	Open Issues and Future Directions	147
4.4	Scenario 4: Complex Financial Networks	147
4.4.1	Threat: Systemic Risk and Cascading Failures	149
4.4.2	Measures of Systemic Risk	150
4.4.3	Countermeasures	152
4.4.4	Open Issues and Future Directions	154
 Part III Infrastructure		
5	Critical Infrastructure	157
5.1	Scenario: Cyberwarfare Targeting Critical Infrastructures	161
5.1.1	Threat: Malware	164
5.1.2	Attacks and Countermeasures	167
5.1.3	Threat: SCADA System Vulnerabilities	173
5.1.4	Attacks and Countermeasures	177
5.1.5	Open Issues and Future Directions	184
5.2	Scenario: A New Cyber-Physical Threat from the Sky	188
5.2.1	Threat: Drones	189
5.2.2	Attacks and Countermeasures	194
5.2.3	Open Issues and Future Directions	195
6	Business Entities	197
6.1	Scenario 1: Unwary Company	198
6.1.1	Threat: Information Gathering	199

6.1.2	Attacks and Countermeasures	204
6.1.3	Open Issues and Future Directions.....	207
6.2	Scenario 2: Infrastructureless Company	210
6.2.1	Threat: Outsourcing of Security.....	212
6.2.2	Attacks and Countermeasures	215
6.2.3	Open Issues and Future Directions.....	225
Bibliography		227
Glossary		245
Index.....		247

List of Figures

Fig. 2.1	Users populating the Web over the years	8
Fig. 2.2	A 5-year summary of the epidemiological data on measles disease in the European region	18
Fig. 2.3	Some of the tweets written by Donald Trump about the climate change and the global warming	23
Fig. 2.4	News consumption of Americans according to the study conducted by journalism.org	26
Fig. 2.5	Categorization of News Content Features and Social Context Features	36
Fig. 3.1	The estimated computational power of the Bitcoin network, expressed in terahashes per second, from its origin to May 2020	84
Fig. 3.2	Market share of the most popular Bitcoin mining pools (June 2020)	86
Fig. 3.3	Global overview of the Bitcoin mining regions. Data sourced from	90
Fig. 3.4	Worldwide distribution of cryptocurrency mining in 2018	92
Fig. 4.1	Total worldwide investment activity in FinTech	100
Fig. 4.2	Top 10 global FinTech deals in 2017, 2018, and 2019	101
Fig. 4.3	The shocking tweet posted by the hacked AP Twitter account in 2013	107
Fig. 4.4	Categorization of the online information sources most used for market prediction	108
Fig. 4.5	Sketch of a successful P&D operation	114
Fig. 4.6	Pyramidal structure of a typical Ponzi scheme	116
Fig. 4.7	The trade-off between performance (i.e., predictive power) and interpretability in machine learning and artificial intelligence algorithms	122
Fig. 4.8	Adversarial examples used to fool computer vision and speech recognition systems.....	123

Fig. 4.9	Categorization of adversarial attacks	125
Fig. 4.10	Number of US banks failed per year, before and after the 2007–2008 Global Financial Crisis	149
Fig. 5.1	Industrial control systems' common multitier security architecture	163
Fig. 5.2	The spread of the WannaCry malware across the globe	168
Fig. 5.3	SCADA systems components and common architecture	174
Fig. 5.4	Industroyer malware architecture	180
Fig. 5.5	Simplified scheme of Industroyer components	181
Fig. 6.1	Intellectual capital of a company	199
Fig. 6.2	Cloud service models	212
Fig. 6.3	DDoS countermeasures.....	224

List of Tables

Table 2.1	Alleged political scandals documented in the literature	27
Table 3.1	Countries that already have or are issuing national or regional cryptocurrencies	72
Table 4.1	Top 10 global FinTech deals in 2017, 2018, and 2019	102
Table 5.1	Most popular malware used to attack critical infrastructure	171
Table 5.2	UAVs classification	191