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

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

List of Figures

List of Tables