Advanced Sciences and Technologies for Security Applications

Babak Akhgar
Ben Brewster *Editors*

Combatting Cybercrime and Cyberterrorism

Challenges, Trends and Priorities

Springer

Advanced Sciences and Technologies for Security Applications

The series Advanced Sciences and Technologies for Security Applications focuses on research monographs in the areas of

- Recognition and identification (including optical imaging, biometrics, authentication, verification, and smart surveillance systems)
- Biological and chemical threat detection (including biosensors, aerosols,materials detection and forensics),

and

- Secure information systems (including encryption, and optical and photonic systems).

The series is intended to give an overview at the highest research level at the frontier of research in the physical sciences.

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

Babak Akhgar · Ben Brewster
Editors

Combatting Cybercrime and Cyberterrorism

Challenges, Trends and Priorities

Springer

Editors
Babak Akhgar
CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research)
Sheffield Hallam University
Sheffield
UK

Ben Brewster
CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research)
Sheffield Hallam University
Sheffield
UK

ISSN 1613-5113 ISSN 2363-9466 (electronic)
Advanced Sciences and Technologies for Security Applications
ISBN 978-3-319-38929-5 ISBN 978-3-319-38930-1 (eBook)
DOI 10.1007/978-3-319-38930-1

Library of Congress Control Number: 2016941287

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Preface

It is with great privilege that we welcome you to the volume *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*. In this collection we provide an authoritative and accessible guide highlighting a broad range of challenges and complexities faced by modern society in relation to cybercrime and cyberterrorism.

At this point, we would like to take the opportunity to recognize the work of the contributors for allowing us to draw upon their expertise in order to shape the content of this book, a process that has enabled us to highlight many of the pressing cyber-related needs and requirements of society within its chapters. This interdisciplinary approach has helped us to bring together a wide range of organizations from large and small-to-medium enterprise, law enforcement and academia to present the reader with an analysis of current and relevant issues pertinent to cybercrime and cyberterrorism.

The growth in significance of cyberspace across society has opened up vectors for, and extended the scope of, many existing forms of criminality. As well as acting as an enabler for the globalization of business, cyberspace has created a truly global landscape for crime as individuals from across the globe are now able to utilize this environment to attack critical national infrastructure, governments and private business by stealing, compromising the integrity of, and destroying data. It has created new market places for the sale and exchange of illegal weapons and drugs, other illicit materials and even the trafficking and exploitation of human beings and provides a platform for the creation and exchange of materials associated with the solicitation and sexual exploitation of children.

However, cyberspace is not only a tool for business and criminal enterprise; citizens increasingly depend on it as a social mechanism, publicly exposing large amounts of information about themselves and those they interact with. For these reasons, it has become vitally important that we address and overcome these new challenges as a society, restoring the confidence we have in the networks and infrastructure that form the backbone of not just European, but global society. Ensuring the future of our economic welfare, privacy and collective security is a

primary concern not limited to the idea of cybercrime. These threats extend beyond extending the reach and scope of traditional criminal motivations through to the emerging threats of cyberterrorism and cyberwarfare. In this context, the very nature of terrorism is evolving because of cyberspace, providing a mechanism for the propagation of ideology and extremist rhetoric, the recruitment, coercion and training of individuals, and a platform to plan and execute attacks against governments, business and critical infrastructure. It is particularly attractive to criminals and terrorists alike due to the potential for anonymity, making the job of investigators and prosecutors to prevent and respond to these activities increasingly difficult.

In response to the growing role cyberspace has across society, both in its ability facilitate new opportunities as well as opening up new threats, this volume covers a wide spectrum of challenges, from analyzing the legal and ethical issues associated with conducting research, to details regarding specific challenge areas such as public/private cooperation, attack attribution and standardization. These subject areas are enriched with contextual information and findings from the research projects contributing to it, providing the theoretical and practical frame for future research, practice and policy aimed at enhancing societal resilience to cyber-threats and contributing towards the overriding objective of supporting initiatives at both national and EU levels. Authored and edited by a multi-disciplinary team of practitioners, researchers and experts from academia, law enforcement and private industry, this new volume provides a welcome introduction to contemporary challenges we face in respect of cybercrime and cyberterrorism, providing a welcome point of reference to aid researchers, practitioners and policy makers in the development of their respective cyber security strategies.

Babak Akhgar
Ben Brewster

Acknowledgement

The editors would like to take this opportunity to thank the multidisciplinary team of contributors who dedicated their time, knowledge and experiences in preparing the chapters contained in this edited volume. In particular, we would like to recognise the dedication of Dr. Raluca-Elena Lefticaru, Constantinos Orphanides, Alison Lyle and the wider team at CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research, Sheffield Hallam University) without whom this edited volume would not have been possible.

We also extend our thanks to the consortium partners of the COURAGE (cybercrime and Terrorism European Research Agenda), CAMINO (Comprehensive Approach to Cyber Roadmap Coordination and Development) and CyberROAD (Development of the Cybercrime and Cyberterrorism Research Roadmap) FP7 Projects for their support of this book:

COURAGE

- Engineering ingegneria informatica
- CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research), Sheffield Hallam University
- European Organisation for Security
- UNICRI (United Nations Interregional Crime and Justice Research Institute)
- Cybercrime Research Institute
- TNO, Netherlands Organisation for applied Scientific Research
- FOI, Swedish Defence Research Agency
- Office of the Police and Crime Commissioner for West Yorkshire
- Aconite Internet Solutions
- EstEnter Polska
- Conceptivity SARL
- Institut Jožef Stefan
- Selex Sistemi Integrati

- Tilburg University
- fraunhofer Gesellschaft
- International Cyber Investigation Training Academy

CAMINO

- ITTI Sp. Z. o. o.
- CBRNE Ltd
- Consiglio Nazionale delle Ricerche
- DFRC AG
- Epsion Ltd
- Everis Aeroespacial y Defensa S.L.
- Universite Montpellier I
- Wyższa Szkoła Policji w Szczytnie
- S21sec Information Security Labs S.L.
- Sec-Control Finland Ltd

CyberROAD

- University of Cagliari, PRA Lab
- Technical University of Darmstadt
- INDRA
- Poste Italiane
- SecurityMatters
- Vitrociset
- FORTH, Foundation for Research and Technology
- INOV – Insec Inovação
- Demokritos National Center for Scientific Research
- SBA Research Austria
- Proprs Ltd.
- NASK, Research and Academic Computer Network
- Polícia Judiciária Portugal
- CEFRIEL Center of Excellence for Research, Innovation, Education and industrial Labs Partnerships
- SUPSI University of Applied Sciences and Arts
- CyberDefcon
- Royal Holloway, University of London
- Greek Ministry of National Defence
- McAfee UK
- MELANI, Reporting and Analysis Unit for Information Assurance

These projects received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration (FP7-SEC-2013) under grant agreement no's 607406 (CAMINO), 607642 (CyberROAD) and 607949 (COURAGE).

Contents

Part I:
Approaching Cybercrime and Cyberterrorism Research

Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research

Bert-Jaap Koops(✉)

TILT Tilburg Institute for Law, Technology, and Society,
Tilburg University, Tilburg, The Netherlands
e.j.koops@tilburguniversity.edu

Abstract. What are grand challenges of cybercrime and cyberterrorism policy and research for the coming one or two decades? To answer this question, we first need to grasp some major trends that influence the future of cybercrime and cyberterrorism, and the combatting thereof, in fundamental ways. This chapter therefore starts with sketching seven megatrends in technology and society: Internet as the infrastructure of everything, autonomic technologies, datafication, the onlife world, the transformation of crime, the fourth generation of cybercrime as attacks on the Internet of Things and People, and the gradual erosion of privacy. Against this background, seven grand challenges for keeping societies secure and inclusive against the threats of CC/CT are presented: underground marketplaces, hiding technologies, ubiquitous data, smart regulation, smart organisation, designing technology, and preserving the human rights framework in a volatile context.

1 Introduction

Cybercrime and cyberterrorism (CC/CT) pose significant challenges to society challenges that are unlikely to decrease in the coming decades. Although much is being done, in policy and practice, to address these challenges, adequate measures remain difficult to conceive and implement, as the field is dynamic, complex, and global. Research is needed to help determine which measures are more likely to be adequate, i.e., both effective and legitimate, not only in the short term but also in the longer run. Policy-makers can, in turn, assist researchers by pointing out which research topics are most urgent and valuable for policy and practice. Thus, policy and research can both benefit from a research agenda that includes those issues that are most pressing to be addressed in public policy to combat CC and CT and that would most profit from high-level research.

Developing policies and research programmes to address the challenges of CC and CT requires insight into the major issues that need to be investigated and addressed. To fulfill this need, the chapters in this book offer an overview

B. Akhgar and B. Brewster (eds.), *Combatting Cybercrime and Cyberterrorism*,
Advanced Sciences and Technologies for Security Applications,
DOI 10.1007/978-3-319-38930-1_1

of significant, topical, and concrete issues and challenges that policy-makers and researchers can or should address. An overview of key issues and topical challenges is not enough, however. In order to be able to prioritise policy measures and research topics, and, perhaps more importantly, to be able to see the larger picture and develop policy and research programmes that are capable of addressing CC/CT challenges also in the longer run. A broader, high-level overview is needed, that shows how the many topics relate to each other and fit the broader landscape of CC/CT policy and research. In that light, this chapter aims to sketch the broader picture that puts the various topics discussed in this book in a wider and longer-term perspective. It is based on experience in CC research and many discussions with researchers, practitioners, and policy-makers over the past two decades, and it is therefore essayistic in character.

What, then, are the grand challenges of CC and CT policy and research for the coming one or two decades? To grasp what the grand challenges are, we can build on known and current challenges in the combating of CC and CT, which are likely to persist in the near future. But we also need some-thing more: a vision of the main trends that are affecting the landscape at large, and which bring along new, or shifted, challenges for policy and research. Major trends that have the potential to change society in fundamental ways are called megatrends, and it is an important exercise to have a timely vision on what today's megatrends are, in order to prepare for the future [13]. Therefore, before listing what is perceived as grand challenges of keeping societies secure and inclusive against the threats of CC/CT, megatrends are mapped that influence the future of CC and CT, and the combating thereof, in fundamental ways.

2 Megatrends

Identified are seven megatrends that have the potential to change the ways in which CC and CT can occur and can be combated. These are perhaps not radically moving away from the current situation, since megatrends take place over a longer period and we are already seeing the first effects of these trends, but they strengthen certain current developments and may require novel responses to the way CC/CT is currently approached in policy, practice and research.

The megatrends can roughly be clustered in two groups. First, we have megatrends taking place at the different layers of the Internet: its infrastructure, its applications, and its content. Second, as a consequence of the trends in the first cluster, we have megatrends associated with changes in society at large, with changes in how crime and terrorism occur in society, and with changes in CC, CT, and how these are combated in particular.

2.1 Megatrend 1: Internet as the Infrastructure of Everything

The Internet is rapidly becoming, or perhaps has in some countries already become, the backbone of everything in society. Not only do communications, media, and entertainment classic functions of the Internet in its earlier days rely