SPRINGER BRIEFS IN CYBERSECURITY

Philippe Baumard

Cybersecurity in France

Springer

SpringerBriefs in Cybersecurity

Editor-in-chief

Sandro Gaycken, European School of Management and Technology (ESMT), Stuttgart, Baden-Württemberg, Germany

Editorial Board

Sylvia Kierkegaard, International Association of IT Lawyers, Highfield, Southampton, UK
John Mallery, Computer Science and Artificial Intelligence, Massachusetts Institute of Technology, Cambridge, MA, USA
Steven J. Murdoch, University College London, London, UK
Kenneth Geers, Taras Shevchenko University, Kyiv, Kievs'ka, Ukraine
Michael Kasper, Department of Cyber-Physical Systems Security, Fraunhofer Institute SIT, Darmstadt, Hessen, Germany

Cybersecurity is a difficult and complex field. The technical, political and legal questions surrounding it are complicated, often stretching a spectrum of diverse technologies, varying legal bodies, different political ideas and responsibilities. Cybersecurity is intrinsically interdisciplinary, and most activities in one field immediately affect the others. Technologies and techniques, strategies and tactics, motives and ideologies, rules and laws, institutions and industries, power and money—all of these topics have a role to play in cybersecurity, and all of these are tightly interwoven.

The SpringerBriefs in Cybersecurity series is comprised of two types of briefs: topic- and country-specific briefs. Topic-specific briefs strive to provide a comprehensive coverage of the whole range of topics surrounding cybersecurity, combining whenever possible legal, ethical, social, political and technical issues. Authors with diverse backgrounds explain their motivation, their mindset, and their approach to the topic, to illuminate its theoretical foundations, the practical nuts and bolts and its past, present and future. Country-specific briefs cover national perceptions and strategies, with officials and national authorities explaining the background, the leading thoughts and interests behind the official statements, to foster a more informed international dialogue.

More information about this series at http://www.springer.com/series/10634

Philippe Baumard

Cybersecurity in France

Springer

Philippe Baumard
Conservatoire National des Arts et Métiers
Paris
France

and

School of Economic Warfare—ESLSCA
Paris
France

ISSN 2193-973X ISSN 2193-9748 (electronic)
SpringerBriefs in Cybersecurity
ISBN 978-3-319-54306-2 ISBN 978-3-319-54308-6 (eBook)
DOI 10.1007/978-3-319-54308-6

Library of Congress Control Number: 2017936344

© The Author(s) 2017
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.

Printed on acid-free paper

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

Foreword

France has always been at the forefront of technological developments in cybersecurity. Its base is in defense and aerospace and its paradigms guiding its sovereignty in security have provided the country with a unique perspective on cybersecurity, supported by great capacities. It started early with strategic thinking and industrial acquisitions in the field, with academic leadership and technology development. Yet France has also been somewhat closed to the outer world with its thoughts and concepts. To a large part, this was intentional. France did not want to share any of its evolution before it reached maturity and much of it was considered national only. Accordingly, most of the activities in aerospace and defense still have not surfaced.

Philippe Baumard has been a part of the history of the field and is an excellent scholar, providing both a first hand account of things and a very thorough, critical, and systematic analysis. This combination is what renders this insight into France so interesting and valuable. It not only opens a window into the mostly secluded activities in France, but also provides a coherent account of histories and causalities of rather universal relevance for any country concerned with strategic cybersecurity. From his accounts on the early history of hacking and IT-security in France, to his systematic analysis of persistent technical issues and the difficulties of possible responses to his political and economic analysis of the underlying issues, the present work provides explanations for many of the hidden and complex mechanisms of the field and develops heuristic frameworks to render them detectable and manageable in the future.

Without question, it will be a must-read for anyone concerned with or interested in the history of cybersecurity or cyberstrategy.

March 2017

Sandro Gaycken
ESMT Berlin

Contents

1 Introduction 1
1.1 The Emergence of Cyber-Domain (1972–2000) 3
1.2 The Rise of Cognitive Warfare (1997–2001) 5
1.3 Early Doctrines of Cognitive Dominance (2001–2005) 9
1.4 The Birth of National Cybersecurity Strategies (2006–2016) 12
References 15

2 A Brief History of Hacking and Cyberdefense 17
2.1 From Defying *Authority* to Defying *Sovereignty* 17
2.2 Exploration Years 19
2.3 Hackers Versus Cyber-Criminals: The Monetization's Years 26
References 30

3 The Determinants of a National Cyber-Strategy 31
3.1 The Nature of Information and Its Constraints on Regulation of Cyber-Defense 31
3.2 Building a National Strategy for Cyber-Defense 34
3.2.1 Anonymity, Attribution and Evidence of Intentionality . . . 36
3.2.2 Attribution of Democratic National Committee's Russian Intrusion 40
3.2.3 Cyber Domain Definition: A "Political" Ontology 47
3.2.4 The Impact of Cybersecurity's Causal Ambiguities on National Policies 49
3.3 The French National Strategy for Cybersecurity 52
3.3.1 An History of Monopoly, Technological Excellence and Fearless Entrepreneurs 52
3.3.2 The Directorate of Information System Security (SCSSI, DCSSI) 1986–2009 55
3.3.3 The Lasbordes (2006) and Romani Reports (2008) 55
3.3.4 The National Defense White Paper of 2008 56

3.3.5 The Creation of ANSSI (2009) . . . 57
3.3.6 The 2010 Cybersecurity Group of the High Council for Strategic Education and Research (CSFRS) . . . 57
3.3.7 The 2011 National Digital Strategy . . . 59
3.3.8 The 2012 Bockel Report on Cyberdefense . . . 60
3.3.9 The 2016 French National Digital Security Strategy . . . 60
References . . . 65

4 National Cyber-Doctrines: Forthcoming Strategic Shifts . . . 67
4.1 Comparing National Cyber-Doctrines . . . 67
4.1.1 Comparing National Strategies . . . 70
4.2 Preventing Cyber-Attacks: Evolution and Technological Shifts . . . 72
4.2.1 A Critical Evolution of Threats: The Fall of the Signature Paradigm . . . 73
4.2.2 The Behavioral Paradigm: Patternless and Intelligent Behaviors . . . 77
4.2.3 Predictive Artificial Intelligence and Incongruity Detection . . . 82
4.2.4 The Elaboration of the First Incongruity Threat Intelligence Model . . . 84
4.3 Exploring Counter-Measures to Defeat AI Campaigns . . . 88
4.3.1 APT Technological Locks and Defensive Strategy Implications . . . 89
4.3.2 Helping Machines to Detect Their Own Incongruous Behaviors . . . 91
4.3.3 The Rise of Artificial Intelligence and Incongruity Detection . . . 92
References . . . 95

5 Conclusion . . . 97
Bibliography . . . 100

Biblioteka Główna
Akademii Sztuki Wojennej
26645/III (CB)
03-026645-000-0

SPRINGER BRIEFS IN CYBERSECURITY

Editor-in Chief: Sandro Gaycke
Series Editors: Sylvia Kierkega

Philippe Baumard

Cybersecurity in Fra

Computer Science

ISBN 978-3-319-54306-2

▶ springer.com