

SPRINGER BRIEFS IN CYBERSECURITY

Myriam Dunn Cavelty

# Cybersecurity in Switzerland



Springer

# **SpringerBriefs in Cybersecurity**

## **Editor-in-Chief**

Sandro Gaycken, Freie Universität Berlin, Berlin, Germany

## **Series editors**

Sylvia Kierkegaard, International Association of IT Lawyers, Southampton, UK

John Mallery, Massachusetts Institute of Technology, Cambridge, MA, USA

Steven J. Murdoch, University of Cambridge, Cambridge, UK

Marco Cova, University of Birmingham, Birmingham, UK

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>

Myriam Dunn Cavelty

# Cybersecurity in Switzerland



Springer

Myriam Dunn Cavelty  
ETH Zürich  
Center for Security Studies  
Zürich  
Switzerland

ISSN 2193-973X ISSN 2193-9748 (electronic)  
ISBN 978-3-319-10619-9 ISBN 978-3-319-10620-5 (eBook)  
DOI 10.1007/978-3-319-10620-5

Library of Congress Control Number: 2014951698

Springer Cham Heidelberg New York Dordrecht London

© The Author(s) 2014

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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media ([www.springer.com](http://www.springer.com))

# Foreword

Myriam Dunn Cavelty's *Cybersecurity in Switzerland* provides an excellent addition to the SpringerBriefs in Cybersecurity series. It is a concise and coherent, well-written summary of the political and strategic process in Switzerland—a small, but tech-savvy and comparatively well-resourced nation. It reflects on the conditions and opportunities of the country, its unique political structure and background underlying the strategic process leading to official documents and initiatives. Many of the cybersecurity approaches of Switzerland are recounted and explained in this way, spanning early discourses on how perceptions and narratives have been formed, to concepts and models, institutions and initiatives, and finally technical and organization implementations. The brief also recounts and evaluates the history of those documents, initiatives, and technologies, pinpointing implementation problems, their causes, and the following evolution of the process. This provides an excellent, history-based insight into learned lessons.

Throughout the Brief Dunn Cavelty also takes a very systematic approach to the topic. Following her insightful historical reflections, thorough theoretical considerations, divide and characterize the processes, assign phases, and identify their structures, requirements and obstacles. With understanding of the principles of cyberstrategy, to reflect and apply in future research or policy making.

In conclusion, this Brief certainly provides a magnificent contribution to the series and the fields of cybersecurity and cyberpolitics. It helps in many ways and I thank the author for a great piece of work.

August 2014

Sandro Gaycken

# Contents

|          |                                                                                 |    |
|----------|---------------------------------------------------------------------------------|----|
| <b>1</b> | <b>Introduction</b>                                                             | 1  |
| 1.1      | The Approach                                                                    | 1  |
| 1.2      | On Terminology                                                                  | 2  |
| 1.3      | Switzerland: A Special Case                                                     | 4  |
| 1.3.1    | Federalism: The Decentralization of Power and Authority                         | 4  |
| 1.3.2    | Consensus Democracy                                                             | 5  |
| 1.4      | Conclusion                                                                      | 6  |
|          | References                                                                      | 6  |
| <b>2</b> | <b>Global Cyber-Security Policy Evolution</b>                                   | 9  |
| 2.1      | Introduction                                                                    | 9  |
| 2.2      | The Undercurrent: Technological Insecurity                                      | 10 |
| 2.3      | Variations of the Cyber-Security Discourse                                      | 12 |
| 2.3.1    | Technical Discourse                                                             | 13 |
| 2.3.2    | Crime-Espionage Discourse                                                       | 14 |
| 2.3.3    | Civil Defense Discourse                                                         | 17 |
| 2.3.4    | Military Discourse                                                              | 20 |
| 2.4      | Conclusion                                                                      | 22 |
|          | References                                                                      | 23 |
| <b>3</b> | <b>The Four-Pillar Model for Information Assurance<br/>(Phase 1: 1997–2004)</b> | 27 |
| 3.1      | Introduction                                                                    | 27 |
| 3.2      | The Day After in Cyberspace ... in Switzerland                                  | 28 |
| 3.2.1    | The SFU 1997                                                                    | 28 |
| 3.2.2    | Aftermath of the SFU 97                                                         | 29 |
| 3.2.3    | Concept Information Assurance 2000                                              | 30 |
| 3.3      | Information Assurance: The Four-Pillar Model                                    | 31 |
| 3.3.1    | Pillar 1: Prevention                                                            | 32 |
| 3.3.2    | Pillar 2: Early Warning                                                         | 34 |

|          |                                                                                                        |           |
|----------|--------------------------------------------------------------------------------------------------------|-----------|
| 3.3.3    | Pillar 3: Damage Limitation . . . . .                                                                  | 34        |
| 3.3.4    | Pillar 4: Combating Causes . . . . .                                                                   | 35        |
| 3.4      | Conclusion . . . . .                                                                                   | 35        |
|          | References . . . . .                                                                                   | 36        |
| <b>4</b> | <b>Reporting and Analysis Center for Information Assurance (MELANI) (Phase 2: 2004–2010)</b> . . . . . | <b>39</b> |
| 4.1      | Introduction . . . . .                                                                                 | 39        |
| 4.2      | Basics of Public–Private Partnerships . . . . .                                                        | 40        |
| 4.2.1    | Win–Win Situations and Trust for Successful Information-Sharing . . . . .                              | 41        |
| 4.2.2    | Mitigating the Obstacles to Public–Private Information-Sharing . . . . .                               | 42        |
| 4.3      | MELANI: The Basic Set-up . . . . .                                                                     | 45        |
| 4.3.1    | The Cooperation Model . . . . .                                                                        | 45        |
| 4.3.2    | Two Customer Bases . . . . .                                                                           | 48        |
| 4.3.3    | Services and Products . . . . .                                                                        | 50        |
| 4.4      | Conclusion . . . . .                                                                                   | 52        |
|          | References . . . . .                                                                                   | 54        |
| <b>5</b> | <b>Consolidation and Cyber-Risk Strategy (Phase 3: 2011–2014)</b> . . . . .                            | <b>57</b> |
| 5.1      | Introduction . . . . .                                                                                 | 57        |
| 5.2      | National Strategy for Critical Infrastructure Protection (2005–2012) . . . . .                         | 58        |
| 5.2.1    | First Report on the Protection of Critical Infrastructures (2007) . . . . .                            | 59        |
| 5.2.2    | Basic Strategy for Critical Infrastructure Protection (2009) . . . . .                                 | 60        |
| 5.2.3    | National Strategy for Critical Infrastructure Protection (2012) . . . . .                              | 62        |
| 5.3      | Cyber-Defense Strategy...or Not (2011–2013) . . . . .                                                  | 63        |
| 5.4      | Cyber-Risk: Reboot! . . . . .                                                                          | 65        |
| 5.4.1    | Cyber-Preparedness in Switzerland . . . . .                                                            | 66        |
| 5.4.2    | The Way Ahead (The “Strategy”) . . . . .                                                               | 69        |
| 5.5      | Conclusion . . . . .                                                                                   | 71        |
|          | References . . . . .                                                                                   | 72        |
| <b>6</b> | <b>Conclusion</b> . . . . .                                                                            | <b>73</b> |
|          | Reference . . . . .                                                                                    | 75        |



# Abbreviations

|         |                                                                          |
|---------|--------------------------------------------------------------------------|
| ARPANET | Advanced Research Projects Agency Network                                |
| BCM     | Business-Continuity Management                                           |
| BSI     | German Federal Office for Information Security                           |
| CCB     | Closed Customer Base                                                     |
| CEO     | Chief Executive Officer                                                  |
| CERT    | Computer Emergency Response Team                                         |
| CI      | Critical Infrastructures                                                 |
| CI/KR   | Critical Infrastructure and Key Resources                                |
| CII     | Critical Information Infrastructures                                     |
| CIIP    | Critical Information Infrastructure Protection                           |
| CIO     | Chief Information Officer                                                |
| CIP     | Critical Infrastructure Protection                                       |
| CIP WG  | Critical Infrastructure Protection Working Group                         |
| CNO     | Computer Network Operations                                              |
| CSIRT   | Computer Security Incident Response Team                                 |
| CSO     | Armed Forces Command Support Organisation                                |
| CYCO    | Cybercrime Coordination Unit Switzerland                                 |
| CySARs  | Suspicious Activity Reports on Cybercrime                                |
| DAP     | Service for Analysis and Prevention (Dienst für Analysis und Prävention) |
| DARPA   | Defense Advanced Research Projects Agency                                |
| DDoS    | Distributed Denial-of-Service Attack                                     |
| DoD     | United States Department of Defense                                      |
| EOC     | Electronic Operations Centre (Swiss Army)                                |
| fedpol  | Swiss Federal Office of Police                                           |
| FIS     | Swiss Federal Intelligence Service                                       |
| FITSU   | Swiss Federal IT Steering Unit                                           |
| FOCP    | Swiss Federal Office of Civil Protection                                 |
| FONES   | Swiss Federal Office for National Economic Supply                        |
| FSUIT   | Swiss Federal Strategy Unit for Information Technology                   |
| GovCERT | Government Computer Emergency Response Team                              |