SPRINGER BRIEFS IN CYBERSECURITY

Martin Schallbruch · Isabel Skierka

Cybersecurity in Germany

Springer

SpringerBriefs in Cybersecurity

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

Martin Schallbruch · Isabel Skierka

Cybersecurity in Germany

Springer

Martin Schallbruch
Digital Society Institute
European School of Management
and Technology
Berlin, Germany

Isabel Skierka
Digital Society Institute
European School of Management
and Technology
Berlin, Germany

ISSN 2193-973X ISSN 2193-9748 (electronic)
SpringerBriefs in Cybersecurity
ISBN 978-3-319-90013-1 ISBN 978-3-319-90014-8 (eBook)
https://doi.org/10.1007/978-3-319-90014-8

Library of Congress Control Number: 2018946668

Printed on acid-free paper

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

Foreword

Germany is certainly one of the more interesting countries when it comes to national cyberpolicies. It has been engaged in data privacy and information security since the very early days of commercial computing. Its federal institutions, crafting and implementing computer security technologies, laws, standards, and rules, are more than twenty years old, and the country's public discourse about privacy and security started in the 1980s and is still very much alive and emotional. And yet while Germany did not really come up with good answers on how to actually solve the cybersecurity problem at large either, it is an interesting place to look at—especially for lessons learned.

But to actually assess lessons learned in Germany, those lessons would have to be marked as such. This is difficult. Germany has a very bad culture regarding errors, especially in the government. There is a saying among German ministries: The ministry never makes a mistake. In other words, if you make a mistake anyhow—which is absolutely inevitable in an area as complex as cybersecurity and rather the rule than the exception—it should still look like a success. That renders learning a tedious and difficult enterprise for those who have not actually been a part of the learning curve.

Lucky for this SpringerBrief, both authors were and are part of the German learning curve and can provide the readers with "inside" insights. Martin Schallbruch and Isabel Skierka are both close participants and watchers of cybersecurity policies in Germany. As former and longtime Ministerial Director of the Federal Ministry of the Interior, Martin Schallbruch has effectively been in charge as both strategist and implementer of most of Germany's previous governmental efforts in cybersecurity. He has overseen the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) and was instrumental in the design of a variety of laws governing cybersecurity in Germany. Now being a scientist, his many firsthand experiences provide a wealth of empirical material on many of the otherwise hidden nuts and bolts of the creation of governance in this area, of wins and losses, imperceptible difficulties, and unearthed options. Isabel Skierka complements this experience with a brilliant and inquisitive scientific mind and her own set of many years of close encounters with cybersecurity policy-making as a governmental advisor and researcher, providing an external perspective. In addition, Isabel Skierka has always been very active in the two other policy fields apart from interior security which were of high relevance in Germany's path in cyberpolicy: defense and foreign policy.

Accordingly, both authors together form a perfect team to describe, analyze, and assess cybersecurity policy-making in Germany, and this is very much reflected in the SpringerBrief.

And they span the entire spectrum of relevant events, structures, perspectives, and actors. They start out by explaining the peculiarities of the German mindset around anything informational and security-based, and the impact these public perspectives had and still have on policy-making. From there, they brilliantly explore the entire history and evolution of Germany's cybersecurity strategy, providing and explaining the main documents, how they came into existence, and how (or in some cases: why not) they have been implemented. These excellent explanations are most valuable as they critically explore the many mundane, yet highly relevant problems stemming from government rivalries, industry influence, and political agendas—elements, which seem negligible to many outsiders, but which actually form the very heart of the lack of progress in many cases of particular policies, initiatives, or technologies. Following these historical explanations, they deepen their systematic analysis of persistent gaps and problems and project their insights on current and evolving policy fields for cybersecurity, some of them again very typically German, predicting (no doubt with high certainty) upcoming problems in the creation of policies for these new areas.

As editor, I am highly pleased and in fact proud of this particular volume, as it does a perfect job at, first, providing an in-depth and otherwise imperceptible look into the hidden secret dynamics of cybersecurity in Germany, and, second, such a brilliant systematic analysis of this particular history, which provides a ton of highly valuable insights for any researcher or practitioner in cybersecurity strategy.

Berlin, Germany
May 2018

Dr. Sandro Gaycken

Contents

SPRINGER BRIEFS IN CYBERSECURITY

Editor-in-Chief: Sandro Gay

Series Editors: Sylvia Kierkeg

Martin Schallbruch · Isabel

Cybersecurity in Germany

Computer Science

ISBN 978-3-319-90013-1
9 783319 900131

▸ springer.com