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

Greg Austin

Cybersecurity in China

The Next Wave

Springer

Greg Austin
Australian Centre for Cyber Security
University of New South Wales
Canberra, ACT
Australia

ISSN 2193-973X ISSN 2193-9748 (electronic)
SpringerBriefs in Cybersecurity
ISBN 978-3-319-68435-2 ISBN 978-3-319-68436-9 (eBook)
https://doi.org/10.1007/978-3-319-68436-9

Library of Congress Control Number: 2018939006

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

China is certainly among the most interesting players in cybersecurity. While oftentimes rather visible as intrusive and offensive, for instance, through its massive efforts to conduct mass surveillance of its own citizens or in its (alleged) global cyber industrial espionage campaigns, the country is also in a rather unique position regarding its defensive cybersecurity outset and interests. It is, by now, heavily industrialized, fully connected, with a large number of foreign companies, bringing their own technologies with them, and its citizens are increasingly more digitalized and connected through the Internet. Accordingly, the country is highly and increasingly vulnerable to cyberattacks or information operations, and strong concerns about its inner and outer security ensue. So strong, in fact, that cybersecurity has been made a senior management priority, with Secretary General Xi Jinping seeing to those matters personally. China in fact considers its cybersecurity a key matter of its sovereignty and keeps stressing its right and duty to create “cyber sovereignty” in many aspects.

The outcome is in many cases very interesting and individual—and of high impact internationally. The close entanglement of technical security, censorship, and surveillance is one example. Another more recent one is the new regulation of foreign companies operating in China. Foreign companies now have to use Chinese security technologies and encryption, encrypted connections are switched off, and even the source code produced or used in China has to be disclosed to the Chinese government. As a result, all these companies will turn more and more transparent. Given China’s interest in industrial espionage, these efforts have been a cause of (mostly silent) outrage abroad and will have wider strategic implications for the Chinese economy—but may also provide a model for other countries striving to achieve cyber sovereignty.

In sum, China is and will continue to be a very interesting place to observe when it comes to the regulation of cybersecurity. Accordingly, it is a great benefit for this SpringerBrief in cybersecurity to have this particular brief about cybersecurity in China, and an even greater benefit to have it written by Greg Austin. Greg is in close touch with China and its cybersecurity regulators for many years, theoretically and practically, and can not only provide a full and credible account of the country's efforts, but also background stories and additional knowledge which can not be found anywhere else. Founded in his competence, this SpringerBrief will help to understand China and its efforts and provide important insights and details for academics, diplomats, and industries alike.

Berlin, Germany
February 2018

Dr. Sandro Gaycken

Preface

China has established a global reputation for cyberattack. How good is it at cyber defense? This book offers a health check, a report card, on China's cybersecurity system in the face of escalating threats from criminal gangs at home and abroad, as well as from hostile states. The book hopes to contribute some new foundations for a comprehensive benchmarking of China's responses to the problem of security in cyberspace. But it cannot claim to offer a comprehensive analysis. The scope of the subject of cybersecurity is simply too broad. In acknowledging that, the book hopes to inform current approaches to assessment of national cybersecurity performance to stimulate more granular research across the broader set of issues that are canvassed in this book.

At a foundational level, the Bell Labs model of cybersecurity distinguishes between eight ingredients of the problem set: software, hardware, networks, payload, power (electricity supply), people, ecosystem, and policy (Rauscher et al. 2006). While each of these may appear at first glance to be relatively compact and bounded for any country, they are individually hugely complex, and have become more so, as technologies like mobile computing, quantum computing, cloud computing, the internet of things (IoT), and advanced artificial intelligence have come into play. Even as understood within the eight-ingredient framework from the engineer's perspective, the field of cybersecurity is highly dynamic.

In defining the boundaries of the subject of cybersecurity according to the eight ingredients, we also need to be cognizant of the different practices, technologies, personnel, and organizations needed for distinct mission sets, such as countering cybercrime against corporations or citizens, online child protection, preventing political subversion, countering cyber espionage, protecting critical infrastructure, and preparing for cyber-enabled warfare.

The subject in this case is China in the broad, but we need to break that down into at least three stakeholder subsets: its government, its corporations, and its citizens. Boundaries between the three sets of subjects in cyber policy and activities are in many circumstances quite fluid. These three sets of stakeholder have many different interests, face many different threats, and have variegated response capabilities.

The three stakeholder sets (each with many subsets) represent fundamentally different social and political phenomena. We must avoid accepting at face value the Chinese government's view that it speaks for cybersecurity in China. It wants to, but as this book demonstrates, it is in the character of the information age that a government cannot be the source of cybersecurity for its corporations or citizens. If we measure government capacity, we are only measuring cybersecurity for the government, not for the country. The Chinese government blurs this distinction, unlike governments in the UK and the USA. These liberal democracies are firmly of the view that the government is not responsible for the cybersecurity of its corporations and citizens when they confront a threat. These two governments limit themselves to providing assistance as they can to non-government actors, both in advance of or during an attack. In most countries, governments have inadequate resources to provide cybersecurity for their own agencies, let alone their corporations and citizens. This stakeholder distinction is becoming more important in China since the central government is proving to be far less capable in delivering cybersecurity for the whole country than it would like to be.

There is a fourth category of stakeholders in Chinese cyberspace: foreign governments, foreign corporations, and foreign citizens. Cybersecurity in the country is an unavoidably international and globalized activity. While this book concentrates on the domestic scene in China, it must also sketch broad outlines of the interaction between Chinese and non-national influences as they take place inside the country.

Thus, the picture presented in the book of cybersecurity in China is a mosaic or a multi-dimensional montage. Conflict between and within the different sets of stakeholders and cybersecurity mission sets in China, as in other countries, is assumed. That said, evidence of the contours of those conflicts in China is often sparse as a result of the country's non-transparent political system.

The contest between and among the different interest groups and mission sets analyzed in this book speaks to the centrality of the concept of power as the ultimate test of national cybersecurity. Many extant measures of cybersecurity at the national level focus on inputs (announced government measures) rather than on results or outcomes (the manifestations of cyber power). This book proposes a new orientation in assessing national cybersecurity: one that relates to the actual exercise of power in cyberspace (the outcomes) in the pursuit of security. In simple terms, the quality of cybersecurity in any country will be defined in larger part by degrees of implementation of policies by a variety of stakeholders, rather than being the sum of policy declarations and intents.

This book is a sequel to *Cyber Policy in China* (Austin 2014), which takes a values-based approach in analyzing China's ambitions of becoming an advanced information society, reviewing political, economic and security aspects, on both the domestic and international fronts. It referenced the many excellent books on cyber censorship and political activism in cyberspace in China that had been written up that time. It also referenced key works on the political economy of China's ICT sector. That book included analysis of the landmark statement by President Xi Jinping in February 2014 that China would do everything needed for the country to become a cyber power. The current book, *Cybersecurity in China*, has a narrower focus on two fronts. First, it has a sharper domestic focus, leaving international considerations somewhat to one side, though not ignoring them completely. Secondly, it focuses exclusively on China's security in cyberspace not its wider "information society" ambition.

This book relies on China's current official definition of cybersecurity, discussed in more detail in Chapter 1. This definition is essentially the same as we might find in other countries—in spite of linguistic preferences around certain renderings of the concept in Chinese. These include: *wǎngluò ānquán*, translated variously by Chinese authors into English as "network security," "cybersecurity," or "cyberspace security"; and *xìnxī ānquán* which is a cognate for the English term "information security." The Chinese approach sees cybersecurity (and/or information security) as a subset of national security. This means that cybersecurity is, for China, as other leading powers, a socio-technical phenomenon: a process or state of mind that seeks to minimize actual and perceived risks to a subject's well-being arising from activities in cyberspace (Austin 2017).

In Chinese scholarship, the socio-technical phenomenon of cybersecurity is a relatively new field of study that takes place in a highly distorted information ecosystem. Universities in the country have been slow to take up the socio-technical dimensions of cybersecurity, and few have dared to undertake critical analysis of politically sensitive aspects of cybersecurity (the larger share of the subject). Leading Chinese studies in the public domain as do exist have been reviewed in preparation of this book.

In scholarship outside China, there are several useful descriptive book-length studies on cybersecurity policy in China published in recent years (ICGC 2012; Ventre 2014; Lindsay et al. 2015; Inkster 2016; Raud 2016; Cheng 2017). In shorter formats, scholars such as Yang Guobin, Adam Segal at the Council on Foreign Relations, Rogier Creemers at Oxford, Nir Kshetri, a group at the Jamestown Foundation (especially Peter Mattis), Joe McReynolds and Leigh Ann Ragland at the Defense Group Inc., Russell Hsiao at Project 2049, the China Media Project at Hong Kong University, and the team at the China Digital Times have regularly made insightful contributions to the body of knowledge on different aspects of China's most recent cybersecurity policies. Similarly strong contributions have been made in a variety of online formats by numerous professionals in foreign ICT corporations and law firms working in or with China. As a result, we know quite well the system for managing the diverse aspects of cybersecurity in China, and the chronological sequence of announced policy responses.

Kshetri (2013: 1) has characterized the general situation well: the "distinctive pattern of the country's cyberattack and cybersecurity landscapes" is explained by "China's global ambition, the shift in the base of regime legitimacy from Marxism Leninism to economic growth, [and] the strong state and weak civil society." One report (Jamestown 2014) observed that "research on Chinese cyber defense lags behind assessment of China's offensive capabilities" and concluded that the resulting approach is "fragmented both by region and function that is further complicated by turf battles between regulators institutions." This book adds contours and depth to such broad assessments offered in shorter formats.

The book also offers an assessment of the effectiveness of efforts in China to protect various interests in cyberspace. In this analysis, the views of Chinese scholars, officials, and other opinion leaders are essential, but through the research for this book, the author formed the view that many key Chinese sources have been ignored in Western scholarship. For a number of reasons, the open-source scholarly study in China of domestic aspects of security in cyberspace as a socio-technical phenomenon is still in its infancy. It has been impossible to verify independently much of the data and many of the claims cited in this book about progress made. At the same time, as some of the material collated in this book suggests, this field of study in China is still substantial enough to be a major source of information and assessment. Moreover, there is a substantial body of knowledge on cybersecurity in China held by market research firms, such as IDC and Gartner, and most scholars do not enjoy easy access to their collections for public citation purposes.

This is the first book on cybersecurity in China to base itself around an assessment of China's cyber industrial complex.

The sequence of chapters is as follows. Chapter 1 provides an introductory snapshot of the cybersecurity ecosystem in China, setting up deeper analysis of subjects raised in later chapters. Chapter 2 provides a review of the state of university-based cybersecurity education in China. Chapter 3 offers a summary of Chinese views of the cyber industrial complex. Chapters 4–6 look in more depth at the actual state of cybersecurity for the three subsets of China called out above: the corporate sector, the citizenry, and the government. Chapter 7 offers an evaluation of the state of cybersecurity in China. A brief Chapter 8, called "The Next Wave," suggests (unsurprisingly) that China's cybersecurity in twenty years' time will look radically different from how it appears today as a result of the policy turns beginning around 2011 and boosted substantially beginning in 2014. But China does not determine its cybersecurity condition alone. This will remain a multi-factor, multi-national enterprise that has to be managed. Given China's choices to oppose the value systems of the US-led liberal democratic alliance, the scope for equanimity for China's leaders in managing cyberspace policy will remain about the same as if they were riding a tiger.

The author would like to thank colleagues in the field, especially from China, who have been open in their discussion of the subjects in this book. The author would also like to acknowledge the support on this project of several part-time research assistants (Lu Wenze, Meng Fei, and Zu Haoyue). The author alone is responsible for analysis and commentary on the material from Chinese language sources provided by the able research assistants, with the several exceptions noted and referenced.

The author is also grateful for permission from The Globalist, the best-informed and most thoughtful daily on the big issues of global affairs, and from The Diplomat, the premier Web site for analysis on Asia-Pacific security affairs, to use his material previously published by them.

Canberra, Australia Greg Austin

References

Austin G (2014) Cyber policy in China. Polity, Cambridge

Austin G (2017) Restraint and governance in cyberspace. In: Burke A, Parker R (eds) Global insecurity: futures of chaos and governance. Palgrave

Cheng D (2017) Cyber dragon. Inside China's information warfare and cyber operations. Praeger, Santa Barbara

ICGC (2012) China and cybersecurity: political, economic, and strategic dimensions. Report from Workshops held at the University of California, San Diego April 2012

Inkster N (2016) China's cyber power. IISS, London

Kshetri N (2013) Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. Electron Commer Res 13:41. https://doi.org/10.1007/s10660-013-9105-4

Lindsay JR, Cheung TM, Reveron DS (eds) (2015) China and cybersecurity: espionage, strategy, and politics in the digital domain. Oxford University Press, Oxford

Raud M (2016) China and cyber: strategies, attitudes and organization. NATO CCDCOE, Tallinn

Rauscher KF, Krock RE, Runyon JR (2006) Eight ingredients of communications infrastructure: A systematic and comprehensive framework for enhancing network reliability and security. Bell Labs Technical Journal 11.3 (2006): 73-81

Ventre D (ed) (2014) Chinese cybersecurity and defense. Wiley

Contents

Acronyms

2FA	Two-Factor Authentication
APT	Advanced Persistent Threat
CAC	Cyberspace Administration of China
CAICT	China Academy of Information and Communications Technology
CAS	Chinese Academy of Sciences
CCP	Chinese Communist Party
CCTV	China Central Television
CEC	China Electronics Information Industry Group (known in English by the acronym CEC for an earlier incarnation, China Electronics Corporation)
CERT	Computer Emergency Response Team
CESI	China Electronic Standards Institute
CETC	China Electronics Technology Group Corporation
CII	Critical Information Infrastructure
CLG	Central Leading Group
CPLC	Central Political and Legal Commission
CNCA	China National Certification Administration
CNCERT/CC	China Computer Emergency Response Team/Coordination Centre
CNITSEC	China National Information Technology Security Evaluation Centre
CNKI	China Knowledge Resource Integrated Database
CNNVD	China National Vulnerability Database for Information Security
CUAA	Chinese Universities Alumni Association
DDOS	Distributed Denial-of-Service
ICT	Information and Communications Technology
ICAO	International Civil Aviation Organization
IEEE	Institute of Electrical and Electronics Engineers
ISOC	Internet Society of China
IT	Information Technology
ITU	International Telecommunications Union

LMS	Lab for Media Search
MIIT	Ministry of Industry and Information Technology
MoE	Ministry of Education
MLPS	Multi-Level Protection System
MPS	Ministry of Public Security
MSS	Ministry of State Security
NICE	National Initiative for Cybersecurity Education
NISSTC	National Information Security Standardization Technical Committee
NPC	National People's Congress
NPU	National Police University
NSA	National Security Agency
OS	Operating System
PLA	People's Liberation Army
PSU	Public Security University
SAR	Special Administrative Region
SCO	Shanghai Cooperation Organization
SEA	State Encryption Administration
SKLOIS	State Key Laboratory of Information Security
SSB	State Secrecy Bureau
TC260	Technical Committee 260
VPN	Virtual Private Network
XJYU	Xian Jiaotong University

List of Tables

List of Boxes