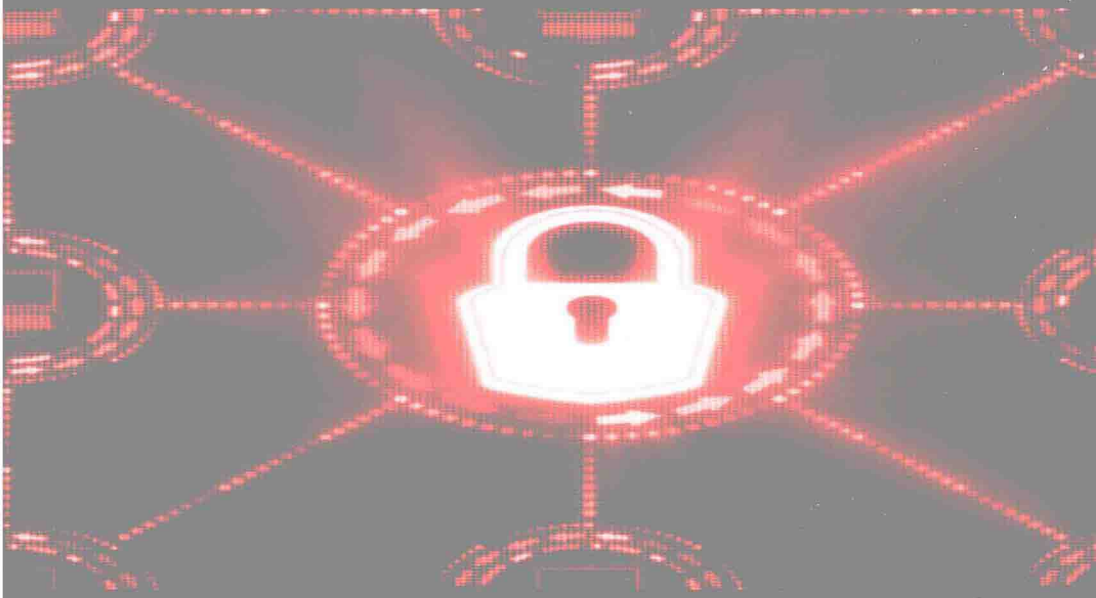
INFORMATION SYSTEMS, WEB AND PERVASIVE COMPUTING SERIES



Chinese Cybersecurity and Defense

Edited by Daniel Ventre

ISTE WILEY

Chinese Cybersecurity and Defense

Edited by

Daniel Ventre

ISTE

WILEY

First published 2014 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

Library of Congress Control Number: 2014941991

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN 978-1-84821-614-3

Printed and bound in Great Britain by CPI Group (UK) Ltd., Croydon, Surrey CR0 4YY

Chinese Cybersecurity and Defense

Author Biographies

Dean Cheng is the Senior Research Fellow for Chinese political and security affairs at the Asia Studies Center of The Heritage Foundation. He specializes in Chinese military and foreign policy, and has written extensively on Chinese military doctrine, technological implications of its space program, and "dual use" issues associated with China's industrial and scientific infrastructure.

Before joining The Heritage Foundation, he was a senior analyst with the Center for Naval Analyses, a federally funded research and development center, and a senior analyst with Science Applications International Corporation (SAIC), the Fortune 500 specialist in defense and homeland security. He has testified before Congress, spoken at the (American) National Defense University, US Air Force Academy, and the National Space Symposium, and been published in the Wall Street Journal and the Washington Post.

Alan Chong is Associate Professor at the S. Rajaratnam School of International Studies in Singapore. He has published widely on the notion of soft power and the role of ideas in constructing the international relations of Singapore and Asia. His publications have appeared in *The Pacific Review*; *International Relations of the Asia-Pacific*; *Asian*

Survey; *East Asia: an International Quarterly*; *Politics, Religion and Ideology*; the *Review of International Studies*; the *Cambridge Review of International Affairs* and *Armed Forces and Society*. He is also the author of *Foreign Policy in Global Information Space: Actualizing Soft Power* (Palgrave, 2007). He is currently working on several projects exploring the notion of 'Asian international theory'. His interest in soft power has also led to inquiry into the sociological and philosophical foundations of international communication. In the latter area, he is currently working on a manuscript titled 'The International Politics of Communication: Representing Community in a Globalizing World'. In tandem, he has pursued a fledgling interest in researching cyber security issues. He has frequently been interviewed in the Asian media and consulted in think-tank networks in the region.

Alice Ekman is Associate Research Fellow in charge of China at the French Institute of International Relations (Ifri), where she conducts analyses of major domestic and foreign policy developments. She is an Adjunct Professor at Sciences Po in Paris, and also lectures at the French Institute for Higher National Defense Studies and the War College. Alice Ekman was formerly Visiting Scholar at Tsinghua University (Beijing), Research Officer at the Embassy of France in China, and Consultant in a Paris-based strategy firm. Fluent in Mandarin Chinese, she regularly undertakes research fieldwork in China and East Asia.

She holds an MA from the London School of Economics in International Relations, Economics, and Anthropology (China focus), and a PhD in International Relations from Sciences Po. Alice Ekman is currently a member of the EU committee of the Council for Security Cooperation in the Asia Pacific (CSCAP).

Thomas Flichy de La Neuville is Professor in international relations at Saint-Cyr military academy. Specialist of Iran, he has studied persian in the National Institute of Oriental Languages an cultures and holds a PhD in legal history. He is visiting professor in Oxford and Annapolis. Amongst his recent publications, *Iran-Russia-China, a new mongol empire?*

Xu Longdi is a PhD and Associate Research Fellow at China Institute of International Studies (CIIS), Beijing. He received his PhD in international relations from the Graduate School of the Chinese Academy of Social Sciences (CASS) in 2009 and joined CIIS the same year. His expertise covers International Relations Theory, international security, and EU politics and foreign policy. Now he runs a program on "International Norms and Cyber Security".

Samuel Cherian is Associate Fellow in the Strategic Technologies Centre at the Institute for Defence Studies and Analysis, an autonomous think tank affiliated to the Indian Ministry of Defence. He has written on various cyber security issues, including critical infrastructure protection, cyber resilience, cybercrime, and internet governance. He has also presented on these topics at seminars and round tables around the world as well as different fora in India. His recent publications include *Cybersecurity and Cyberwar*, (October 2013 issue of *Seminar* magazine), *Emerging Trends in Cyber Security*, (IDSA Web Comments March 28, 2012), and *Prospects for India-US Cyber Security Cooperation*, (Volume 31, Issue 2, Strategic Analysis September 2011). His monograph *Global, Regional and Domestic Dynamics of Cybersecurity* will be published shortly. He was co-ordinator of the IDSA Task Force on Cyber Security which published a report on "*India's Cyber Security Challenges*" in March 2012.

He holds a PhD from the Jawaharlal Nehru University, New Delhi.

Daniel Ventre holds a PhD in Political Science (University of Versailles). He is the Secretary General of GERN (*Groupe Européen de Recherches sur les Normativités – European Research Group into Norms*), researcher at CESDIP (*Center for Sociological Research on Law and Criminal Justice Institutions. CNRS / University of Versailles / Ministry of Justice*), Chairholder in Cyber Security & Cyber Defense (*Saint-Cyr / Sogeti / Thales*). He is the author of a number of books and articles (published in French, English and Chinese) on cyberwarfare, information warfare, cyberconflict, cybersecurity and cyberdefense. He has published:

Information Warfare – 信息战, National Defense Industry Press, Beijing, 218 pages, January 2014.
Cyber Conflicts, Competing National Perspectives, ISTE, London and John Wiley & Sons, New York, May 2012, 330 pages.
Cyberwar and Information Warfare, ISTE, London and John Wiley & Sons, New York, July 2011, 448 pages.
Cyberattaque et Cyberdéfense, Paris, Editions Hermès Lavoisier, Collection "Cybercriminalité et Cyberconflits", August 2011, 312 pages.
Cyberespace et acteurs du cyberconflit, Paris, Hermès Lavoisier, Collection "Cybercriminalité et Cyberconflits", April 2011, 288 pages.
Cyberguerre et guerre de l'information. Stratégies, règles, enjeux, Paris, Hermès Lavoisier, Collection "Cybercriminalité et Cyberconflits", September 2010, 318 pages.
Information Warfare, ISTE, London and John Wiley & Sons, New York, 2009, 298 pages.
La guerre de l'information, Paris, Hermès Lavoisier, Collection "Finance Gestion Management", 2007.

Introduction

Regardless of the origins of cyberspace (those who designed it, the founding fathers of computing, of telecoms, of the Internet, the first to give financial backing to these projects, etc.), what is important to look at in today's world is the current configuration of cyberspace, and its possible future. Whilst a map of the under-sea cable networks shows the Internet as being rather US-centered, or at least organized around the triad of the USA, Europe and Asia, with the other regions of the world appearing to lie on the periphery, this centrality of infrastructures (root name servers, computation capacities, data flux, etc.), but also of investment, research, users, etc., is in the full throes of evolution. Technology and knowledge are now being disseminated throughout the world. Where it is impossible to install hardwired technologies quickly enough, mobile telephony is becoming an important means of access to the Internet. Poorer populations are beginning to gain access to a Web connection. Thus, modern technologies are able to make their effects felt even in territories where they are not as omnipresent as in the United States. The technology is becoming more widely available, and we can see that the barriers to development are not economic or technical, but often political: the development of cyberspace, and the form

Introduction written by Daniel VENTRE.

that it takes, are subject to the will of the political authorities.

Whilst the United States still seem, at present, to be the dominant force in terms of the Internet and cyberspace, the more widely the technology propagates, the less the number of users is concentrated in the Western World. This evolution of cyberspace is contributing to the current shift of power (economic, political and strategic power) from America toward Asia. The report "The World in 2025"[1] affirms (and it is not alone in doing so) that "the centre of gravity of world production will move towards Asia [...] Before 2025 China could become the second world economic power". This shift is not solely economic. It runs deeper, corresponding to the shifting of the very foundations of the power of modern nations: "*Before 2025 China could become the second world economic power [...] India and China could thus account for approximately 20% of the world's R&D*". The configuration of cyberspace is constantly changing as well. There is no truly stable balance. The same report highlights the effects this evolution will inevitably have: "*If the United States remain the first military power, the scientific and technological catching-up of some states, the new irregular war tactics and the increasing importance of cyber-attacks will weaken their freedom of action*".

Although, evidently, the domination of cyberspace (particularly in economic, political and military terms) depends on more factors than simply the number of users in a state (there are other variables determining the power balance in cyberspace: political goals, industrial expertise, capital, knowledge, data, infrastructure, the capacity to impose a strategy on all three levels of cyberspace), the evolution of uses and populations of users represents a major phenomenon,

1 European Commission, *The World in 2025. Rising Asia and Socio-Ecological Transition*, Brussels, 2009, 28 pages, [http://ec.europa.eu/research/social-sciences/pdf/the-world-in-2025-report_en.pdf].

because it also reflects the changing desires, political, economic and ideological projects. This evolution reflects, or perhaps heralds, a gradual transfer of power from one center (the United States) to another (China). China is, without a doubt, the major player in this reconfiguration. The stakes are enormously high, because if, tomorrow, the 1.5 billion Chinese were all to have access to the Internet, the configuration of China's cyberspace itself and of the world as a whole, would be turned on its head. In cyberspace, Asia is becoming the most important resource in terms of users, consumers, citizens, but also (potentially at least) of creators, designers, although innovation in these domains appears, as yet, to be concentrated in Silicon Valley and in Israel (notably in the domain of cybersecurity). The center of innovation, in the field of ICTs, could, in time, be shifted from America, with its giants of industry and research, to Asia. Even at this stage, China has already developed its own solutions – alternatives to the tools employed in the West (Facebook, Twitter, operating systems, etc.), and its industrial players (e.g. Huawei and Lenovo) are in the process of dethroning the historical international market leaders. By exporting its technologies, and investing in the development of infrastructure in developing countries, China is also creating the conditions for future dependency on its technologies. No doubt China will also be able to invest wisely in technologies with a promising future – e.g. those which will feed into the up-and-coming "Internet of Things" – firstly because of its immense national market, but also because engineers, who are already digital natives, constitute a potential creative resource. In addition, a billion or more Chinese citizens in cyberspace also represent phenomenal quantities of data produced. It is a crucial focal point for authorities, companies and even states to be able to cope with these amounts of data. The capacities to innovate, invest and deploy one's technologies throughout the world constitute as many variables of importance for the power of modern states. Asia, and particularly China, intends to play the leading roles in these domains.

When thinking about the issues of cyberspace, its influence on the quality of international relations and on the evolution of the world, and looking at the importance of cyber strategies for national and international equilibria, China is naturally at the center of the debate. The questions are numerous: what are the variables affecting Chinese power? What is China's ambition – what role does it hope to play on the international stage? In what ways can its society and its political regime evolve? How does cyberspace fit in with these issues of both internal and international politics? What will be the consequences of the evolution of cyberspace and of its use, for Chinese society, for other countries in the region, and for the rest of the world? Are the proposals formulated and the initiatives taken by China in terms of governance of the Internet able to reshape the interconnection of the world such as it is imagined and defined by the West? The evolution of cyberspace, with the central role that China now plays and will continue to play for a long time to come, is now a matter of security and national defense. Cybersecurity and cyberdefense are political and strategic issues of prime importance. Practices, intentions and projects in this field have a direct influence on international relations. New actors, new forms of relations between states, new powers, conflicts and power distributions are taking shape throughout cyberspace.

The aim of this book is to analyze China's policies, strategies and practices in the area of cybersecurity and cyberdefense; and also to analyze the effect they have on the political and strategic choices made by other states. Contributions to this work have come from seven researchers, specializing in international relations and issues of cybersecurity. The individual chapters are drawn from a conference which took place in Paris, on 1 July 2013, organized by the *Chair of Cyberdefense and Cybersecurity* (Saint-Cyr / Sogeti / Thales).

Contents