

INFORMATION SYSTEMS, WEB AND PERVASIVE COMPUTING SERIES



Chinese Cybersecurity and Defense

Edited by Daniel Ventre

ISTE

WILEY

Chinese Cybersecurity and Defense

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.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms and licenses issued by the CLA. Enquiries concerning reproduction outside these terms should be sent to the publishers at the undermentioned address:

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

© ISTE Ltd 2014

The rights of Daniel Ventre to be identified as the author of this work have been asserted by him in accordance with the Copyright, Designs and Patents Act 1988.

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

Contents

AUTHOR BIOGRAPHIES	xi
INTRODUCTION	xv
CHAPTER 1. CHINA’S INTERNET DEVELOPMENT AND CYBERSECURITY – POLICIES AND PRACTICES	1
Xu LONGDI	
1.1. Introduction.	1
1.2. Internet development in China: an overview	2
1.3. China’s policies towards Internet development	5
1.3.1. From the very beginning of its development, China’s Internet has been closely linked to the Chinese economy, and was programmed and integrated into its macro economic development blueprints	6
1.3.2. In addition to lending full policy support to Internet development, China also invests heavily in building Internet infrastructures.	8
1.3.3. The Chinese government actively promotes the R&D of next-generation Internet (NGI).	8
1.3.4. China practices a policy of managing cyber affairs in line with law, adhering to the principles of scientific and effective administration in its Internet governance	9
1.4. Cyber legislation and Internet administration	9
1.4.1. Basic principles and practices of Internet administration in China	10

1.4.2. Guaranteeing the free and secure flow of information in cyberspace.	16
1.5. Cybersecurity and diplomacy: an international perspective	27
1.5.1. Cyber policy dialogue and consultation	28
1.5.2. Regional cyber cooperation	30
1.5.3. Track II cyber diplomacy	32
1.5.4. Legal cooperation in combating cybercrimes.	33
1.5.5. Technical cooperation	35
1.5.6. Office for Cyber Affairs of the MFA.	40
1.6. A cybersecurity strategy in the making?	41
1.6.1. Significance of the Internet for China	45
1.6.2. Goals and objectives	45
1.6.3. Cyber threat landscape	45
1.6.4. Means for strategic goals.	48
1.7. Conclusion.	53
CHAPTER 2. PLA VIEWS ON INFORMATIONIZED WARFARE, INFORMATION WARFARE AND INFORMATION OPERATIONS	55
Dean CHENG	
2.1. The evolution of chinese military thinking	56
2.2. The growing importance of information	59
2.3. Information operations	64
2.3.1. Command and control missions	65
2.3.2. Offensive information missions	66
2.3.3. Defensive information missions	70
2.3.4. Information support and safeguarding missions	71
2.4. Key types of information operations	72
2.4.1. Electronic combat (dianzizhan; 电子战).	72
2.4.2. Network combat (wangluozhan; 网络战).	73
2.4.3. Psychological combat (xinlizhan; 心理战).	74
2.4.4. Intelligence combat (qingbaozhan; 情报战)..	75
2.4.5. Command and control combat (zhihuikongzhizhan; 指挥控制战).	76
2.4.6. Physical combat.	78
2.5. Computer network warfare and information operations	79

CHAPTER 3. CHINA’S ADAPTIVE INTERNET MANAGEMENT STRATEGY AFTER THE EMERGENCE OF SOCIAL NETWORKS		81
Alice EKMAN		
3.1. Weibo: the turning point		82
3.1.1. Adaptive behaviors		82
3.1.2. Participative behaviors.		87
3.2. Latest adjustments under Xi Jinping		89
3.2.1. Smart management of the Internet: a top priority under the new leadership.		89
3.2.2. “Guiding public opinion”...		96
3.2.3. ...while seizing economic opportunities		97
3.3. Bibliography		99
 CHAPTER 4. INDIA’S CYBERSECURITY – THE LANDSCAPE		 101
Cherian SAMUEL		
4.1. A snapshot of Asian cyberspace.		102
4.1.1. Aspects of cyberconflict in Asia		106
4.1.2. West Asia		106
4.1.3. East Asia		110
4.2. The Indian cyber landscape		114
4.3. The China challenge: a case study		117
4.4. Responses		121
4.4.1. Implementing a national cybersecurity policy.		121
4.5. Creating an institutional framework		123
4.5.1. Ensuring supply chain integrity.		124
4.6. Takeaways		126
 CHAPTER 5. CHINA AND SOUTHEAST ASIA: OFFLINE INFORMATION PENETRATION AND SUSPICIONS OF ONLINE HACKING – STRATEGIC IMPLICATIONS FROM A SINGAPOREAN PERSPECTIVE		 129
Alan CHONG		
5.1. Offline sphere: latent “diasporic” information power and official Chinese soft power		133
5.2. The online sphere: hacktivism as mostly projections		149

5.3. Conclusion: offline politics strategically obscure online projections	152
5.4. Bibliography	153

**CHAPTER 6. IMPACT OF MONGOLIA'S CHOICES IN
INTERNATIONAL POLITICS ON CYBERSECURITY 157**
Daniel VENTRE

6.1. Mongolia's cyberspace	158
6.2. Cyberspace and political stakes.	160
6.2.1. Mongolia targeted by cyber-attacks.	160
6.2.2. Nationalism on the Internet.	167
6.3. Information-space security policy.	168

**CHAPTER 7. CHINA-IRAN-RUSSIA – A CYBERCOMMUNITY
OF INFORMATION? 177**
Thomas FLICHY DE LA NEUVILLE

7.1. The hall marks of cyber-cooperation.	178
7.1.1. Pax cyber-mongolica.	178
7.1.2. A cyber-community of information – the proof of Syria.	179
7.1.3. The counter-point of Mali	180
7.2. The geopolitical bases for the cyber-mongol empire	181
7.2.1. An undeniable closer Sino-Iranian relationship.	182
7.2.2. Arms sales in Russo-Iranian and Sino-Iranian relations.	184
7.2.3. Sino-Russian support for Iranian civil nuclear development	186
7.2.4. A clear-cut Sino-Russian diplomatic position on the Iranian program.	187
7.2.5. Oil and gas at the heart of economic relations.	190
7.3. Order in cyberspace: an absolute necessity within China	194
7.3.1. Interior order and exterior disorder.	194
7.3.2. The appearance of peace and the necessity of secrecy.	196

CHAPTER 8. DISCOURSE REGARDING CHINA: CYBERSPACE AND CYBERSECURITY	199
Daniel VENTRE	
8.1. Identification of prevailing themes	203
8.1.1. Depictions of the Internet in China.	203
8.1.2. Impact of cyberspace on Chinese society	207
8.1.3. The Chinese cyber threat	214
8.1.4. The Chinese army: its practices, capabilities and strategies	223
8.1.5. Espionage.	228
8.1.6. China, cyberspace and international relations . . .	240
8.1.7. Particular points from the Western perspective . .	244
8.2. The evolution of American discourse about China, cybersecurity and cyber defense	247
8.2.1. The annual reports of the US Defense Department	248
8.2.2. Speeches of the Secretaries of Defense.	263
8.2.3. Prospective analyses conducted by the National Intelligence Council.	272
8.3. Conclusion.	277
GENERAL CONCLUSION	283
LIST OF AUTHORS.	295
INDEX.	297

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 and 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.