
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