

Table of Contents

Introduction	ix
Daniel VENTRE	
List of Acronyms	xvii
Chapter 1. Cyberwar and its Borders	1
François-Bernard HUYGHE	
1.1. The seduction of cyberwar	2
1.2. Desirable, vulnerable and frightening information	4
1.3. Conflict and its dimensions	6
1.4. The Helm and space	8
1.5. Between knowledge and violence	11
1.6. Space, distance and paths	13
1.7. The permanency of war	16
1.8. No war without borders	22
1.9. The enemy and the sovereign	25
1.10. Strengths and weaknesses	27
1.11. Bibliography	29
Chapter 2. War of Meaning, Cyberwar and Democracies	31
François CHAUVANCY	
2.1. Introduction	31
2.2. Informational environment, a new operating space for strategy	34
2.2.1. War and information: stakes for the West	35
2.2.2. Strategy in the information environment	44
2.2.3. Winning the battle of legitimacies	52
2.3. Influence strategy: defeating and limiting armed force physical involvement	59

2.3.1. Describing the aggressor.	60
2.3.2. Armed forces and the information environment	65
2.3.3. The need for moral force	70
2.4. Conclusion	78
2.5. Bibliography	79

Chapter 3. Intelligence, the First Defense? Information Warfare and Strategic Surprise 83

Joseph HENROTIN

3.1. Information warfare, information and war.	85
3.2. Intelligence and strategic surprise.	90
3.2.1. Strategic surprise	91
3.2.2. Perception of surprise	94
3.2.3. Perception of the possibility of surprise.	95
3.3. Strategic surprise and information warfare	98
3.4. Concluding remarks: surprise in strategic studies	106
3.5. Bibliography	109

Chapter 4. Cyberconflict: Stakes of Power 113

Daniel VENTRE

4.1. Stakes of power	113
4.1.1. Power relations	116
4.1.2. Expression of sovereignty	154
4.1.3. Cyberpower	155
4.1.4. Measuring and locating power	159
4.1.5. Limits of exercising power	175
4.1.6. The Monroe doctrine.	179
4.1.7. Globalization	181
4.1.8. Shock theories.	181
4.1.9. Naval and maritime power strategy	184
4.1.10. Air/space and cybernetic power: analogies	194
4.1.11. Cyberconflict/cyber weapons, chemical/biological weapons: comparisons	203
4.1.12. Cyberconflict/cyber weapons, Cold War, nuclear weapons: comparisons	204
4.1.13. Cyberconflict and new wars.	213
4.2. The Stuxnet affair	230
4.3. Bibliography	240

Chapter 5. Operational Aspects of a Cyberattack: Intelligence, Planning and Conduct 245

Eric FILIOL

5.1. Introduction. 245

5.2. Towards a broader concept of cyberwar 247

5.2.1. War and cyberwar: common ground. 247

5.2.2. New orders in cyberwar 249

5.2.3. Who are cyberwarriors? 252

5.2.4. Is formalization possible? 253

5.3. Concept of critical infrastructure 253

5.3.1. Generalized definition of the notion of critical infrastructure 254

5.3.2. System interdependence 257

5.4. Different phases of a cyberattack 260

5.4.1. Intelligence phase. 260

5.4.2. Planning phase 266

5.4.3. Conduct phase. 267

5.5. A few “elementary building blocks” 268

5.5.1. General tactical framework 268

5.5.2. Attacks on people. 270

5.5.3. Opinion manipulation and area control 271

5.5.4. Military computer attack in a conventional operation 273

5.6. Example scenario 273

5.6.1. Tactical scenario 274

5.6.2. The order of events 277

5.6.3. Analysis 278

5.7. Conclusion 281

5.8. Bibliography 282

Chapter 6. Riots in Xinjiang and Chinese Information Warfare 285

Daniel VENTRE

6.1. Xinjiang region: an explosive context 287

6.1.1. Ethnic tensions, extremism, separatism, terrorism and violence in Xinjiang 287

6.1.2. Xinjiang: a strategic region 291

6.2. Riots, July 2009 291

6.2.1. Chronology of facts 291

6.2.2. Reasons for the riots 295

6.2.3. The riots faced with international public opinion 297

6.3. Impacts on Chinese cyberspace: hacktivism and site defacing. 303

6.3.1. The Internet in Xinjiang: a region dependent on information systems? 303

6.3.2. Website defacement in a crisis context 305

6.3.3. Defining the dynamics of the relationship between “political events” and “site defacement”	309
6.4. Managing the “cyberspace” risk by the Chinese authorities	339
6.4.1. Inaccessible sites	339
6.4.2. Cutting off telephone communications	344
6.4.3. The risks of cyberspace	345
6.4.4. Dealing with the media and information content	351
6.4.5. After the incidents: communication, reaction, control, legislation	353
6.5. Chinese information warfare through the Xinjiang crisis	354
6.5.1. Xinjiang, land of information warfare	355
6.5.2. Chinese information warfare in the prism of Xinjiang management crisis approaches	356
6.6. Conclusion	361
6.7. Bibliography	364
Chapter 7. Special Territories	367
Daniel VENTRE	
7.1. Hong Kong: intermediate zone	367
7.1.1. Strategic and political situation in Hong Kong	367
7.1.2. Hong Kong’s cyberspace	369
7.1.3. A framework suited to crises	371
7.1.4. Hong Kong’s vulnerable cyberspace	373
7.1.5. The Google affair	377
7.2. North Korea: unknown figure of asymmetrical threat	379
7.2.1. Cyberattacks blamed on North Korea	381
7.2.2. North Korea’s capability in cyberwar	385
7.2.3. The Cheonan affair	388
7.2.4. In the face of North Korea: the capabilities of South Korea	390
7.3. Bibliography	393
Conclusion	395
Daniel VENTRE	
List of Authors	401
Index	403