Table of Contents

Abbreviations xi

Introduction xvii

Chapter 1. The United States 1

1.1 Information warfare in the 1990s 1
1.1.1. Points of view from security experts 1
1.1.2. US Air Force doctrine: AFDD 2-5 (1998) 6
1.1.3. The doctrine of the Joint Chiefs of Staff committee: JP 3-13 (1998) 8
1.1.4. Components of information warfare 11
1.2. Information warfare in the 2000s 19
1.2.1. Dictionary of the Department of Defense 19
1.2.2. US Air Force: AFDD 2-5 (2005) and AFPD 10-7 (2006) 19
1.2.3. The doctrine of the Joint Chiefs of Staff committee: JP 3-13 (2006) 21
1.3. Other important concepts and reflections 23
1.3.1. Cyberspace and superiority of information 23
1.3.2. The “value” of information 26
1.3.3. Information system 29
1.3.4. Command and control warfare: C2W 30
1.3.5. Effect-Based Operations (EBOs) 31
1.3.6. Information-in-warfare 32
1.3.7. The OODA loop 32
1.3.8. Fourth generation warfare 33
1.3.9. Noosphere 35
1.3.10. RMA 35
1.3.11. C4ISR 37
1.3.12. Network centric warfare (NCW) 38

1.3.13. ISR: intelligence, surveillance, reconnaissance 39
1.3.14. Cyberwar 40
1.3.15. Netwar 40
1.3.16. Spin doctoring 41
1.3.17. Intelligence 41
1.3.18. Information operations 42
1.4. Loss of information control 44
1.5. American concerns 50

Chapter 2. China 53

2.1. The concept of "information warfare": a genesis 54
2.1.1. General Wang Pufeng: one of the pioneers 54
2.1.2. Colonel Wang Baocun 56
2.1.3. Colonels Qiao Liang and Wang Xiangsui: out of bounds war. . . . 57
2.1.4. General Dai Qingmin and Wang Baocun 62
2.1.5. General Niu Li, Colonel Li Jiangzhou and Major Xu Dehui 63
2.1.6. 2004 white book on national defense 64
2.1.7. Sun Tzu and information warfare 66
2.1.8. How to implement the theories 68
2.2. The American perspective on Chinese information warfare, modernization and informatization of the PLA 71
2.2.1. Interpretation problems 72
2.2.2. The impenetrability of China 72
2.2.3. Information warfare 74
2.2.4. Why is China intensifying the modernization of its armies?. 81
2.2.5. Technologies for army modernization. 83
2.2.6. In search of interpretations: the concept of "shashoujian" 87
2.2.7. 2008 DoD report concerning Chinese military power 89
2.3. Relations between Beijing and Taipei 102
2.3.1. The assassin's mace against the strategy of the scorpion. 104
2.3.2. Cyber-attacks against Taiwan: psychological effects 104
2.3.3. Taiwan and information warfare 106

Chapter 3. India 109

3.1. Entry into information society 109
3.1.1. Has India entered the age of information? 110
3.1.2. Security of information systems 111
3.2. Information warfare: development and adoption of the doctrine 112
3.2.1. The military doctrine. 112
3.2.2. Official parties 119
3.2.3. Adoption of the information warfare doctrine 121
3.3. Understanding attacks against Indian cyberspace 124

3.3.1. Indian site defacements: statistics. 124
3.3.2. Cyber crime or acts of aggression/acts of war? 129
3.4. Indian hackers 132

Chapter 4. Japan. 133

4.1. Japanese cyberspace flaws 133
4.1.1. Theft of defense classified data. 133
4.1.2. Loss/theft of sensitive or confidential data 141
4.2. The challenges of cyberspace security 146
4.2.1. Relations between civilian and the military worlds 146
4.2.2. Cyber crime or act of information warfare? 146
4.2.3. Optimal security? 147
4.2.4. The challenges of non-traditional security 147
4.3. Information warfare: a specific Japanese approach?. 150

Chapter 5. Russia 155

5.1. Estonia–Russia: information warfare? 155
5.1.1. Reconstitution of facts 155
5.2. Doctrines and components of the “information warfare” concept. . . . 161
5.2.1. The development of the Russian military. 162
5.2.2. Intellectual information warfare 168
5.2.3. Control of an individual’s physical dimensions 170
5.3. Potential players of information warfare. 171
5.3.1. Government agencies 171
5.3.2. The military 172
5.3.3. Hackers. 173
5.4. The Russia–Georgia conflict: new information warfare? 173
5.4.1. Operations in Russian and Georgian cyberspace 174
5.4.2. The introduction of “cyberwar” and “information warfare” in the conflict. 176
5.4.3. Comments on “cyber attacks” 177
5.4.4. Isolated cyber attacks or information warfare operations? 185
5.4.5. Formulating the right questions 187

Chapter 6. Singapore 191

6.1. Regional and global economic ambition. 191
6.2. Challenges to security. 193
6.3. Cyberspace and national security 194
6.3.1. Protected computers 195
6.3.2. Terrorism. 195
6.3.3. Internet content as a source of threat 196

6.3.4. Data-mining to help security 198
6.4. Singapore armed forces in the information age 200
6.4.1. Towards modernization of armies 200
6.4.2. IKC2: Singapore's version of network centric warfare 201
6.5. Players in information warfare 202
6.5.1. Defense sector agencies 202
6.5.2. Universities and defense 204
6.5.3. Training for information warfare 205
6.6. International cooperation and cyberspace protection 205

Chapter 7. Identifying Aggressors and Acts of Aggression 209

7.1. Statistical data 214
7.1.1. China: CNCERT/CC reports 215
7.1.2. Hong Kong: HKCERT/CC report 219
7.1.3. Japan: JPCERT/CC reports 220
7.1.4. South Korea: KrCERT/CC 2005 report 221
7.2. Attacks against personal information and information warfare 224
7.2.1. Characteristics of attacks against personal information 224
7.2.2. Personal data in information warfare 238
7.2.3. Attacks against personal data as a method of aggression 239
7.3. Classification of CNA type aggressions 241
7.3.1. Problems and limitations of attacks 241
7.3.2. Methods of attacks 243
7.3.3. being able to define the origin of attacks with accuracy? 243
7.4. The players in CNA type aggressions 244
7.4.1. The hacker 247
7.4.2. The sponsors 249
7.4.3. Targets 250
7.5. One weapon amongst others: the virus 250
7.6. Understanding the possible strategies of attackers 252
7.6.1. Use of information warfare 252
7.6.2. Stigmergy 253
7.6.3. Swarming 254
7.6.4. Open source models as a guerilla warfare model 255
7.6.5. Psychological maneuvers or how to lie on a grand scale 256
7.6.6. The role of Internet sites in information warfare 262
7.6.7. Using blogs? 262
7.6.8. Website defacement and semantic attacks 263
7.6.9. What is cyber terrorism? 266
7.6.10. Use of web applications by insurgents 273
7.6.11. Questioning the relations between political context and cyber attacks 275

Chapter 8. An Information Warfare Law? 279

8.1. Warfare and the law 280
8.2. Engaging in and conducting a war 281
8.3. Protecting combatants and non combatants 282
8.4. The challenges of information warfare for international law 284

Conclusion 287

Bibliography 293

Index 301