

---

## Contents

---

<b>Introduction</b> . . . . .	ix
<b>Chapter 1. The United States</b> . . . . .	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) . . . . .	7
1.1.3. The doctrine of the Joint Chiefs of Staff committee: JP 3-13 (1998). . . . .	10
1.1.4. Components of information warfare . . . . .	14
1.2. Information warfare in the 2000s. . . . .	23
1.2.1. Dictionary of the Department of Defense . . . . .	23
1.2.2. US Air Force: AFDD 2-5 (2005) and AFPD 10-7 (2006). . . . .	24
1.2.3. The doctrine of the Joint Chiefs of Staff committee: JP 3-13 (2006) . . . . .	26
1.3. Information warfare in the 2010s. . . . .	28
1.4. Important concepts and reflections. . . . .	43
1.4.1. Information operations . . . . .	44
1.4.2. Information superiority . . . . .	51
1.4.3. The “value” of information. . . . .	62
1.4.4. Information system . . . . .	65
1.4.5. Command and control warfare: C2W. . . . .	66
1.4.6. Effect-based operations (EBOs). . . . .	68
1.4.7. The OODA loop . . . . .	69
1.4.8. RMA. . . . .	70

1.4.9. C4ISR . . . . .	72
1.4.10. Network centric warfare (NCW) . . . . .	73
1.4.11. ISR: intelligence, surveillance, reconnaissance. . . . .	74
1.4.12. Cyberwar . . . . .	75
1.4.13. Netwar. . . . .	89
<b>Chapter 2. China</b> . . . . .	<b>91</b>
2.1. Significant publications. . . . .	91
2.2. Strategic and doctrinal thinking about information warfare. Genesis. . . . .	96
2.2.1. General Wang Pufeng: one of the pioneers . . . . .	97
2.2.2. Wang Baocun and Li Fei . . . . .	100
2.2.3. Wei Jincheng . . . . .	104
2.2.4. Colonels Qiao Liang and Wang Xiangsui: unrestricted warfare . . . . .	105
2.2.5. General Dai Qingmin and Wang Baocun . . . . .	111
2.2.6. General Niu Li, Colonel Li Jiangzhou and Major Xu Dehui. . . . .	114
2.2.7. 2004 White Paper on national defense . . . . .	115
2.3. Recent policies and strategies on information and cyber security . . . . .	117
2.3.1. The Science of Military Strategy 2013 . . . . .	118
2.3.2. Defense White Paper 2013 . . . . .	118
2.3.3. Sino-Russian cybersecurity agreement 2015 . . . . .	119
2.3.4. <i>PLA Daily</i> editorial on 20 May 2015 . . . . .	121
2.3.5. Defense White Paper of 26 May 2015. . . . .	122
2.3.6. The national cybersecurity bill of July 2015 . . . . .	125
2.4. Reflections . . . . .	125
2.4.1. The American perspective on Chinese information warfare, modernization and informatization of the PLA . . . . .	125
2.4.2. Evolution of analyses and discourse about Chinese strategy. . . . .	163
2.4.3. China as a “victim”. . . . .	172
2.4.4. The strategy of active defense . . . . .	173
<b>Chapter 3. Russia</b> . . . . .	<b>177</b>
3.1. Military doctrines and national security strategies . . . . .	180
3.2. Information warfare in practice . . . . .	185
3.2.1. Cyber attacks against Estonia. Who is the culprit? . . . . .	186

3.2.2. The Russia–Georgia conflict . . . . .	194
3.2.3. Ukraine . . . . .	214
3.3. Comments . . . . .	220
3.3.1. Characteristics of the Russian idea of information warfare . . . . .	220
3.3.2. Aggressiveness . . . . .	222
3.3.3. Type of Cold War . . . . .	223
3.3.4. Challenges, objectives and targets . . . . .	224
3.3.5. Psychological information warfare . . . . .	229
3.3.6. Players of information warfare . . . . .	233
3.3.7. Hybrid warfare and information warfare. . . . .	236
3.3.8. Information warfare: what is new... . . . .	240
<b>Chapter 4. Concepts and Theories: Discussions . . . . .</b>	<b>247</b>
4.1. Doctrines . . . . .	247
4.2. Information warfare: definitions, models . . . . .	256
4.2.1. The information environment . . . . .	257
4.2.2. Definitions and models for information warfare . . . . .	261
4.3. Information warfare or data warfare? . . . . .	281
4.3.1. Defining data . . . . .	284
4.3.2. Some theories about data . . . . .	289
4.3.3. Visualization . . . . .	296
4.3.4. Data warfare? . . . . .	306
<b>Conclusion . . . . .</b>	<b>325</b>
<b>Index . . . . .</b>	<b>329</b>