Contents

List of abbreviations and concepts —— XIII

Introduction —— 1

1 The PRC and People’s Liberation Army —— **1**
2 China’s rise —— **9**
3 Economically liberal, politically closed: Chinese “cyberwarfare” and strategic culture —— **11**
4 China’s military rise: the 1991 Gulf War and the genesis of PLA thinking on “cyberwar” —— **14**
5 PLA reforms and restructuring PRC Security Ministries —— **16**
6 Chinese cyberespionage prior to 2015: 3PLA, 4PLA, and the TRBs —— **19**
7 Unit 61398 —— **21**
8 The Ministry of State Security —— **23**
9 Chinese cyberespionage and their tactics, techniques, and procedures —— **26**
10 The lawfulness of cyberespionage —— **28**
11 Traditional intelligence gathering, espionage, and cyberespionage —— **31**
12 Cyberwarfare through pre-positioning in CI —— **34**
13 9/11: Counterterrorism priorities but increasing state threats —— **36**
14 Structure —— **41**

Chapter 1
Decoding the dragon: Chinese theories of cyberespionage and cyberwarfare —— 44

1 Introduction —— **44**
2 Mirror imaging: a note of caution —— **44**
3 Information Warfare and the PLA —— **47**
4 Unrestricted Warfare —— **49**
5 Acupuncture or paralysis warfare: “The supreme art of war is to subdue the enemy without fighting” —— **53**
6 Shen Weiguang and Total Information War —— **56**
7 The 2001 Science of Military Strategy —— **64**
8 The 2001 SMS and Strategic Psychological War —— **67**
9 The “Three Warfares” and SPW: The theories of Dai Qingmin prior to 2003 —— **68**
10 “Winning without fighting”: PLA theories and the 2003 Second Gulf War —— **72**
11 Dai Qingmin: Paralysis/Acupuncture Warfare (2005) —— **74**

12 Cyberespionage and pre-positioning for cyberwar: PLA theories, 2006–2010 —— **76**
13 Moving from theory to practice: cyber deterrence, Stuxnet, and “catch-up”, 2011–2014 —— **78**
14 The 2013 Science of Military Strategy —— **80**
15 Reform and reorganization: China’s 2015 military strategy —— **82**
16 From informatized to intelligentized warfare, 2015–2020 —— **86**
17 AI, cyber innovation, and renewed reorganization, 2020–2024 —— **94**
18 PLA research, education and China’s military-civilian universities —— **97**
19 “Picking flowers in foreign lands to make honey in China”: Chinese academia in Western universities —— **101**
20 Leveraging China’s domestic universities —— **104**
21 Conclusion —— **106**

Chapter 2
China: critical infrastructure pre-positioning and holding it “at risk” —— 110
1 Introduction —— **110**
2 From theory to practice: Chinese hacking —— **111**
3 Chinese reconnaissance and pre-positioning within critical infrastructure —— **113**
4 “Name and Shame” or “hack back”? —— **115**
5 Chinese cyberespionage campaigns and targets —— **117**
5.1 “Titan Rain” and early cyber operations —— **118**
5.2 “Night Dragon” —— **119**
5.3 Comment Crew/APT1 and Telvent —— **120**
5.4 “Operation Aurora” and “Elderwood” —— **123**
5.5 “Shady Rat” —— **125**
5.6 The OPM breach, 2013–2015 —— **126**
5.7 Volt Typhoon —— **131**
6 Attribution —— **135**
7 The formation of the PLASSF: cyber reserve forces and cyber militias, 1995–2015 —— **136**
8 Leveraging supercomputing, quantum computing, Machine Learning, and Artificial Intelligence —— **141**
9 Chinese ventures in Western critical infrastructure —— **144**
9.1 DJI Science and Technology in the U.S. —— **144**
9.2 Huawei and core telecommunications infrastructure —— **147**
9.3 ZTE —— **150**
9.4 Civil nuclear power in the UK —— **151**
9.5 Firmware and chip-level vulnerabilities —— **154**

10 Chinese vulnerability to critical infrastructure attack — 155
10.1 China's underlying telecommunications infrastructure — 162
10.2 Crisis management in China — 166
11 Conclusion — 170

Chapter 3
Chinese intellectual property theft: "the greatest transfer of wealth in history" — 172
1 Introduction — 172
2 Hacking to order? — 174
3 Chinese cyberespionage, HUMINT, and supply chains — 177
4 Chinese counterintelligence and counterespionage — 179
5 New bottles but old wine — 182
6 China's rationale and shifting intelligence priorities in the U.S. as an enabler of cyberespionage — 186
7 "The greatest transfer of wealth in history": IP theft in the defense-industrial base — 187
8.1 China's military-industrial targets — 191
8.2 Su Bin and aerospace hacking — 193
8.3 Civilian targets: AMSC and Sinovel — 197
8.4 Civil-military targets: Trelleborg Offshore — 200
8.5 Reverse engineering — 201
9 The 2015 Obama–Xi agreement — 204
10 Continuing attacks: attribution and attempts at "naming and shaming" — 208
11 Conclusion — 209

Chapter 4
IP theft, military modernization, and China's rise — 213
1 Introduction — 213
2 China's rise in a changing world — 214
3 The Belt and Road Initiative: National development, "soft power", and cyberespionage — 218
4 Chinese soft power and hard-power "alliances" — 222
5 Chinese conventional forces — 225
6 The PLAAF: reengineering stolen IP — 228
7 The PLAN: Coastal protection, guarding the BRI, and "blue water" power projection — 232
8 The PLARF: missile and missile capabilities — 241
9 Space denial: satellites, ASAT, A2/AD, and C^2 — 248

10 “Thucydides’ Trap”? China’s military posture and “gunboat diplomacy” —— 254
11 Conclusion —— 260

Final conclusions —— 264
1 PLA structure, restructuring, and Chinese intelligence —— 266
2 From unrestricted warfare to seizing information supremacy —— 271
3 From theory to practice: cyberespionage, pre-positioning, and holding critical infrastructure “at risk” —— 276
4 China: a cyber threat, a rising power, and an opportunity to engage —— 281
5 China’s universities and private sector —— 290
6 Intelligence and counterintelligence —— 293
7 The Chinese Dream —— 296
8 Sino-Russian dialogues: military-politico cooperation, intelligence sharing, and agreements —— 299
9 Great power rivalry and gray areas —— 306

Appendix —— 311
Sources —— 317

Bibliography —— 318
Books —— 318
Book chapters —— 322
Journal articles —— 324
Mainstream news sources (newspaper reports, magazines, and periodicals) —— 332
Original Chinese sources —— 344
Government hearings, reports, submissions, sources, statements, and alerts —— 346
U.S. Justice Department indictments —— 353
United Nations reports —— 354
Military reports —— 355
Think tank, intergovernmental, and non-governmental organization sources —— 355
Industry reports —— 364
Websites —— 366

Index —— 372