

Contents

<i>List of Figures</i>	<i>page</i> x
<i>Acknowledgments</i>	xi
1 Introduction	1
1.1 What Does Conquest Mean in Cyberspace?	4
1.2 Précis	10
2 Hostile Conquest as Information Warfare	15
2.1 An Ideal-Type Definition of Information Warfare	16
2.1.1 Control at One Layer Is Not Control at Another	24
2.1.2 Applying the Ideal-Type Definition	27
2.2 There Is No Forced Entry in Cyberspace	31
2.3 Information Warfare Only Looks Strategic	37
2.3.1 IW Strategy and Terrorism	43
2.4 Conclusions	49
3 Information Warfare as Noise	50
3.1 Disinformation and Misinformation	51
3.2 Defenses against Noise	55
3.2.1 Redundancy	55
3.2.2 Filtration	57
3.3 What Tolerance for Noise?	59
3.3.1 Tolerance in Real Environments	60
3.3.2 Castles and Agoras	62

vi	<i>Contents</i>	
	3.3.3 Hopping from Agoras to Castles?	64
	3.3.4 Castling Foes	66
	3.4 Concluding Observations	71
4	Can Information Warfare Be Strategic?	73
	4.1 Getting In	75
	4.2 Mucking Around	79
	4.2.1 Spying	79
	4.2.2 Denial of Service	80
	4.2.3 Corruption	81
	4.2.4 Distraction	83
	4.3 Countermeasures	84
	4.3.1 Redundancy	84
	4.3.2 Learning	85
	4.4 Damage Assessment	87
	4.5 Prediction	90
	4.5.1 Intelligence Is Necessary	90
	4.5.2 Intelligence Alone Is Hardly Sufficient	93
	4.6 Is Information Warfare Ready for War?	95
	4.6.1 The Paradox of Control	96
	4.6.2 Other Weaponization Criteria	97
	4.7 Conclusions	100
5	Information Warfare against Command and Control	102
	5.1 The Sources of Information Overload	103
	5.1.1 Its Effect on Conventional Information Warfare Techniques	105
	5.2 Coping Strategies	107
	5.2.1 Who Makes Decisions in a Hierarchy?	107
	5.2.2 Responses to Information Overload	111
	5.3 Know the Enemy's Information Architecture	116
	5.3.1 Elements of Information Culture	117
	5.3.2 Elements of Nodal Architecture	118
	5.3.3 Injecting Information into Adversary Decision Making	118
	5.4 Ping, Echo, Flood, and Sag	121

	<i>Contents</i>	vii
	5.4.1 Ping and Echo	121
	5.4.2 Flood and Sag	122
	5.5 Conclusions	124
6	Friendly Conquest in Cyberspace	125
	6.1 A Redefinition of Conquest	126
	6.2 The Mechanisms of Coalitions	128
	6.2.1 The Particular Benefits of Coalitions	130
	6.2.2 Information and Coalitions	131
	6.2.3 The Cost of Coalitions in Cyberspace	136
	6.3 Enterprise Architectures and Influence	142
	6.4 Alliances with Individuals	148
	6.4.1 The Special Case of Cell Phones	151
	6.5 Alliances of Organizations	155
	6.5.1 Ecologies of Technological Development	155
	6.5.2 DoD's Global Information Grid (GIG)	159
	6.5.3 Merging the Infrastructures of Allies	164
	6.6 Conclusions	166
7	Friendly Conquest Using Global Systems	169
	7.1 Geospatial Data	170
	7.1.1 Coping with Commercial Satellites	175
	7.1.2 Manipulation through Cyberspace	178
	7.1.3 Getting Others to Play the Game	180
	7.1.4 Some Conclusions about Geospatial Services	182
	7.2 National Identity Systems	182
	7.2.1 Two Rationales for a National Identity System	183
	7.2.2 Potential Parameters for a Notional System	184
	7.2.3 Constraints from and Influences over Foreign Systems	187
	7.3 Compare, Contrast, and Conclude	191
8	Retail Conquest in Cyberspace	193
	8.1 Information Trunks and Leaves	194
	8.2 Where Does Cheap Information Come From?	195
	8.3 Surveillance in Cyberspace	198

viii	<i>Contents</i>	
8.4	Making Information Global	203
8.5	Privacy	204
8.6	Amalgamating Private Information	206
8.7	Using the Information	208
8.7.1	General Coercion	208
8.7.2	Specific Coercion	209
8.7.3	Persuasion	211
8.8	Some Limits of Retail Warfare in Cyberspace	214
8.9	Using Retail Channels to Measure Wholesale Campaigns	215
8.10	Conclusions	218
9	From Intimacy, Vulnerability	220
9.1	Do the Walls Really Come Down?	220
9.2	Intimacy as a Target	222
9.3	The Fecklessness of Friends	225
9.4	Betrayal	228
9.5	Conclusions	230
10	Talking Conquest in Cyberspace	231
10.1	Four Layers of Communications	232
10.1.1	Human Conversation in Layers	232
10.1.2	Cyberspace in Layers	236
10.2	Complexity Facilitates Conquest	240
10.2.1	Complexity and Hostile Conquest	241
10.2.2	Complexity and Friendly Conquest	242
10.3	Semantics	245
10.4	Pragmatics	249
10.5	Lessons?	255
11	Managing Conquest in Cyberspace	256
11.1	Conducting Hostile Conquest in Cyberspace	257
11.2	Warding Off Hostile Conquest in Cyberspace	262
11.2.1	Byte Bullies	262
11.2.2	Headless Horsemen	265
11.2.3	Perfect Prevention	268

<i>Contents</i>	<i>ix</i>
11.2.4 Total Transparency	270
11.2.5 Nasty Neighborhoods	272
11.3 Exploiting Unwarranted Influence	276
11.4 Against Unwarranted Influence	281
11.4.1 In Microsoft’s Shadow	282
11.4.2 Microsoft and Computer Security	285
11.5 Conclusions	289
Appendix A: Why Cyberspace Is Likely to Gain Consequence	291
A.1 More Powerful Hardware and Thus More Complex Software	292
A.2 Cyberspace in More Places	294
A.3 Fuzzier Borders between Systems	297
A.4 Accepted Cryptography	299
A.5 Privatized Trust	301
A.6 The Possible Substitution of Artificial for Natural Intelligence	303
A.7 Conclusions	306
<i>Index</i>	307