

Contents

Acknowledgments.....	v
About the Authors.....	xv
About the Technical Editor.....	xvii
Foreword.....	xix
Introduction.....	xxiii
CHAPTER 1 What is Cyber Warfare?.....	1
What is Cyber Warfare?.....	1
Definition for Cyber Warfare	2
Tactical and Operational Reasons for Cyber War.....	4
Cyber Strategy and Power.....	5
Cyber Arms Control.....	7
What is the United States Doing About the Threat of a Cyber War?.....	9
Have We Seen a Cyber War?.....	12
Case Studies	13
The Debate (Is it Real?).....	15
Why Cyber Warfare is Important.....	15
Summary	16
Endnotes.....	17
CHAPTER 2 The Cyberspace Battlefield.....	19
Boundaries in Cyber Warfare.....	19
Defense in Depth.....	20
Physical Infrastructure.....	21
Organizational View.....	22
Where Cyber Fits in the War-fighting Domains	26
Land.....	26
Sea	27
Air.....	27
Space	28
Cyber Domain	28
Threatscape	29
Most Active Threats	29
Most Dangerous Threats	30
Motivations.....	32
Fielding Systems at the Speed of Need.....	34
Summary	35
Endnotes.....	36

CHAPTER 3	Cyber Doctrine.....	37
	Current U.S. Doctrine	37
	U.S. Forces	39
	U.S. Air Force	39
	U.S. Navy	40
	U.S. Army	40
	DoD INFOCONs.....	41
	Sample Doctrine/Strategy from Around the World	43
	Chinese Doctrine	43
	Other Key Nations Developing Doctrine	44
	Translating Traditional Military Doctrine.....	46
	IPOE	46
	JMEM.....	47
	MOE	47
	BDA	48
	CAS	48
	COIN	48
	Guidance and Directives	49
	CNCI	49
	DHS	49
	HSPD.....	50
	NIST	52
	Academia and Industry Associations	53
	Operations and Exercises	54
	Federal Exercises.....	55
	DoD Exercises.....	55
	Educational Exercises.....	56
	Sample MESLs.....	56
	Summary	57
	Endnotes.....	57
CHAPTER 4	Cyber Warriors	61
	What Does a Cyber Warrior Look Like?	61
	Certifications	62
	Education and Training	63
	Experience and Skills	64
	Differences from Traditional Forces.....	66
	Age	66
	Attitude.....	66
	Physical Condition	67
	Credentials.....	68

Present Cyber Warfare Forces	69
U.S.....	69
China	71
Russia	71
France	71
Israel.....	72
Brazil	72
Singapore.....	72
South Korea.....	72
North Korea.....	73
Australia	73
Malaysia	73
Japan.....	73
Canada	74
United Kingdom.....	74
Other Countries with Cyber Forces.....	74
Corporate	74
Criminal.....	75
Staffing for Cyber War.....	76
Sources of Talent.....	76
Training the Next Generation.....	77
Summary	80
Endnotes	80
CHAPTER 5 Logical Weapons	83
Reconnaissance Tools	84
General Information Gathering	85
Whois	87
DNS	88
Metadata	90
Maltego.....	93
Defense.....	94
Scanning Tools.....	94
Nmap	95
Nessus.....	97
Defense	100
Access and Escalation Tools.....	100
Password Tools	101
The Metasploit Project	102
Immunity CANVAS.....	104
Defense.....	105

Exfiltration Tools	106
Physical Exfiltration	106
Encryption and Steganography	107
Using Common Protocols	107
Out of Band Methods	108
Defense	108
Sustainment Tools	109
Adding “Authorized” Access	109
Backdoors	109
Defense	110
Assault Tools	110
Meddling with Software	110
Attacking Hardware	112
Defense	113
Obfuscation Tools	113
Location Obscuration	113
Log Manipulation	114
File Manipulation	115
Defense	116
Summary	117
Endnotes	118

CHAPTER 6 Physical Weapons 119

How the Logical and Physical Realms are Connected	120
Logical Systems Run on Physical Hardware	120
Logical Attacks Can Have Physical Effects	121
Infrastructure Concerns	122
What is SCADA?	123
What Security Issues are Present in the World of SCADA?	124
What are the Consequences of SCADA Failures?	125
Supply Chain Concerns	126
Compromised Hardware	126
Deliberately Corrupted Components	127
Non-Technical Issues	128
Tools for Physical Attack and Defense	128
Electromagnetic Attacks	129
Covert Activity	132
Summary	136
Endnotes	137

CHAPTER 7	Psychological Weapons	139
	Social Engineering Explained	139
	Is Social Engineering Science?	140
	SE Tactics Techniques and Procedures (TTPs)	140
	Types of SE Approaches	142
	Types of SE Methodologies	143
	How the Military Approaches Social Engineering	145
	Army Doctrine.....	146
	How the Military Defends Against Social Engineering.....	149
	How the Army does CI.....	151
	An Air Force Approach.....	151
	Summary	152
	Endnotes	152
CHAPTER 8	Computer Network Exploitation.....	155
	Intelligence and Counter-Intelligence	156
	Sources of Cyber Attacks	156
	Attackers and Sponsors of Attacks.....	157
	Reconnaissance	157
	Open Source Intelligence	157
	Passive Reconnaissance	159
	Surveillance.....	161
	Justifications for Surveillance	161
	Advanced Persistent Threat.....	162
	Voice Surveillance	163
	Data Surveillance	163
	Large-Scale Surveillance Programs	164
	Uses of Surveillance Data	165
	Summary	165
	Endnotes	166
CHAPTER 9	Computer Network Attack.....	167
	Waging War in the Cyber Era.....	168
	Physically	168
	Electronically.....	168
	Logically.....	169
	Reactively vs. Proactively	169
	Time as a Factor	170
	The Attack Process.....	170
	Recon.....	171
	Scan	172

Access.....	173
Escalate.....	174
Exfiltrate	174
Assault.....	175
Sustain	177
Obfuscate.....	177
Summary	178
Endnotes.....	178
CHAPTER 10 Computer Network Defense	179
What We Protect	180
Confidentiality, Integrity, Availability	181
Authenticate, Authorize, and Audit.....	182
Security Awareness and Training	183
Awareness	184
Training	185
Defending against Cyber Attacks.....	185
Policy and Compliance.....	186
Surveillance, Data Mining, and Pattern Matching	187
Intrusion Detection and Prevention.....	187
Vulnerability Assessment and Penetration Testing.....	188
Disaster Recovery Planning	188
Defense in Depth.....	189
Summary	190
Endnotes.....	191
CHAPTER 11 Non-State Actors in Computer Network Operations.....	193
Individual Actors.....	194
Script Kiddies.....	195
Malware Authors.....	195
Scammers	196
Blackhats	196
Hacktivists.....	197
Patriot Hackers	197
Corporations.....	197
Motivation for Corporations to Act in Cyber Warfare.....	198
Cyber Terrorism	198
Reasons for Cyber Terrorist Attacks.....	199
What Will Happen When We See a Cyber Terrorist Attack?.....	199
Organized Cyber Crime	201
Motivations for Criminal Organizations	201

Autonomous Actors	202
Exploratory Systems	202
Attack Systems	203
Defensive Systems	204
Summary	205
Endnotes	206
CHAPTER 12 Legal System Impacts	207
Legal Systems	209
International	210
United States Laws	211
Criminal Law	212
Key U.S. Laws	213
International Trafficking in Arms Regulations	214
U.S. Cyber Related Laws	214
Privacy Impacts	218
Electronic Communications Privacy Act	218
Digital Forensics	219
Certification	221
Summary	222
Endnotes	222
CHAPTER 13 Ethics	225
Ethics in Cyber Warfare	226
Use of Force	226
Intent	227
Secrecy	227
Attribution	227
Military Ethics	227
Bellum Iustum (Just War Theory)	228
Jus ad Bellum (The Right to Wage War)	230
Jus in Bello (Proper Conduct in War)	232
Jus Post Bellum (Justice after War)	234
Summary	235
Endnotes	236
CHAPTER 14 Cyberspace Challenges	239
Cybersecurity Issues Defined	240
Policy	241
Processes	242
Technical	243

Skills	247
People	247
Organization	249
Core (Impacting All Areas)	249
Interrelationship of Cybersecurity Issues	252
Way Ahead	254
Summary	255
Endnotes	256
CHAPTER 15 The Future of Cyber War	257
Near Term Trends	263
Most Likely and Most Dangerous Courses of Action	266
New Technologies and New Problems	268
International Interactions	270
Summary	271
Endnotes	271
Appendix: Cyber Timeline	273
Index	277