

Contents

<i>List of Figures and Tables</i>	ix
<i>Acknowledgments</i>	xi
1 Introduction	1
HERBERT LIN <i>and</i> AMY ZEGART	
2 Illuminating a New Domain: The Role and Nature of Military Intelligence, Surveillance, and Reconnaissance in Cyberspace	19
CHRIS INGLIS	
3 How Effects, Saliencies, and Norms Should Influence U.S. Cyberwar Doctrine	45
HENRY FARRELL <i>and</i> CHARLES L. GLASER	
4 A Strategic Assessment of the U.S. Cyber Command Vision	81
MAX W. E. SMEETS <i>and</i> HERBERT LIN	
5 A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning	105
AUSTIN LONG	
6 Second Acts in Cyberspace	133
MARTIN C. LIBICKI	

7	Hacking a Nation's Missile Development Program	151
	HERBERT LIN	
8	The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities	173
	JASON HEALEY	
9	The Cyber Commitment Problem and the Destabilization of Nuclear Deterrence	195
	ERIK GARTZKE <i>and</i> JON R. LINDSAY	
10	Cyber Terrorism: Its Effects on Psychological Well-Being, Public Confidence, and Political Attitudes	235
	MICHAEL L. GROSS, DAPHNA CANETTI, <i>and</i> DANA R. VASHDI	
11	Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications	265
	STEVEN M. BELLOVIN, SUSAN LANDAU, <i>and</i> HERBERT LIN	
12	Rules of Engagement for Cyberspace Operations: A View from the United States	289
	C. ROBERT KEHLER, HERBERT LIN, <i>and</i> MICHAEL SULMEYER	
13	U.S. Offensive Cyber Operations in a China-U.S. Military Confrontation	319
	ADAM SEGAL	
14	Disintermediation, Counterinsurgency, and Cyber Defense	343
	DAVID AUCSMITH	
15	Private Sector Cyber Weapons: An Adequate Response to the Sovereignty Gap?	357
	LUCAS KELLO	
16	Cyberwar Inc.: Examining the Role of Companies in Offensive Cyber Operations	379
	IRV LACHOW <i>and</i> TAYLOR GROSSMAN	
	<i>Index</i>	401
	<i>Contributors</i>	417

Figures and Tables

Figure 4-1	Main Observation Underlying U.S. Cyber Command's 2018 Vision	89
Figure 4-2	Potential Trade-Offs in Objectives for U.S. Cyber Command	90
Figure 4-3	Win/Win Scenarios for U.S. Cyber Command	92
Figure 4-4	Escalation (Win/Lose and Lose/Lose) Scenarios for U.S. Cyber Command	94
Figure 11-1	An Attack on a Target "I," Passing through "J" and "K"	277
Figure 11-2	An Attack on a Target "I," Passing through "J" and "K," but Where "A" and "B" Rely on "I" for Their Own Functions	278
Table 4-1	U.S. Cyber Command in Numbers	84
Table 4-2	Comparison of Vision I and Vision II of U.S. Cyber Command	86
Table 9-1	Cyber Operations and Crisis Stability	222

Table 10-1	Stress and Anxiety Measures Following a Cyber Terror Attack	246
Table 10-2	Threat Perception Measures Following Experimental Cyber Terror Attacks	247
Table 10-3	Confidence Measures, Study 2 (Hamas)	249
Table 10-4	Political Action Following Cyberattack on Selected Facilities	250
Table 10-5	Support for Domestic Cyber Policy and for Retaliatory Cyber Policy in Response to a Cyber Terror Attack	251
Table 10-6	Risk Assessment of Different Types of Cyber Terror Attacks Perpetrated by Hamas	254
Table 15-1	Passive versus Active Defense in the Cyber Domain	363