

Contents

<i>List of Tables</i>	x
<i>Preface</i>	
<i>Gary Chapman, Diego Latella and Professor Carlo Schaefer</i>	xi
<i>Notes on the Contributors</i>	xiii
<i>Glossary</i>	xvii

Part I: Cyberwar, Netwar and the Revolution in Military Affairs: Defining the Issues

1 Defining the Issues	3
<i>Dr Philippa Trevorrow, Dr Steve Wright, Professor David Webb and Dr Edward Halpin</i>	
2 Virtual Violence and Real War: Playing War in Computer Games: The Battle with Reality	12
<i>Martin Bayer</i>	
2.1 Introduction	12
2.2 Gaming platforms	13
2.3 Definition and historical context	15
2.4 Computer game genres	17
2.5 Realism versus reality	21
2.6 Games and professional military simulations	25
2.7 Conclusion	27
3 Strategic Information Warfare: An Introduction	32
<i>Gian Piero Siroli</i>	
3.1 Introduction	32
3.2 Context	33
3.3 Critical infrastructures	35
3.4 Vulnerabilities	37
3.5 Actors: how and who	41
3.6 Open questions and comments	43
3.7 Conclusions	45

Part II: Implications of the Problem

4	Virtuous Virtual War	51
	<i>Jari Rantapelkonen</i>	
4.1	Introduction	51
4.2	Theory, information technology and accident	52
4.3	War on terrorism – the state of emergency	55
4.4	The necessity and problematics of an enemy	56
4.5	War on Afghanistan – from postmodern moments to information isolation	58
4.6	Battle for the strategic truth	60
4.7	War on Iraq – differences in perceptions	61
4.8	The fog of peace	67
5	Risks of Computer-Related Technology	72
	<i>Dr Peter G. Neumann</i>	
5.1	Introduction	72
5.2	Roles of technology	78
6	Missile Defence – The First Steps Towards War in Space?	82
	<i>Professor David Webb</i>	
6.1	The military use of space	82
6.2	Anti-satellite (ASAT) programmes	84
6.3	Current US developments	87
6.4	Missile defence	89
6.5	The possibility of space weapons control	92
7	Technology as a Source of Global Turbulence?	98
	<i>Dr Stefan Fritsch</i>	
7.1	Introduction	98
7.2	Realistic and neorealistic approaches to technology	99
7.3	Interdependent globalism	100
7.4	Technology and IR/IPE from a constructivist point of view	102
7.5	Arguments for a broader perspective on technology	103
7.6	Multidimensional effects of technology	104
7.7	Conclusion	106
8	Nuclear Weapons and the Vision of Command and Control	113
	<i>Dr Bruce D. Larkin</i>	
8.1	The White House and the Department of Defense (DoD)	114
8.2	The White House Communications Agency	115

8.3	Crisis experience: the attempted assassination of President Ronald Reagan	116
8.4	Crisis experience: The September 11 attack	117
8.5	The Global Command and Control System (GCCS) (as defined by the DoD)	119
8.6	GCCS-T: the top secret provision for nuclear operations	120
8.7	Ongoing transformation of command and control systems	121
8.8	War experience: the Iraq War (2003–...)	123
8.9	Is GCCS sufficiently reliable for nuclear operations?	124
8.10	Is SIPRNET sufficiently secure for nuclear operations?	125
8.11	Assessment	130
9	Information Warfare and the Laws of War	139
	<i>Geoffrey Darnton</i>	
9.1	Introduction	139
9.2	Information Warfare (IW)	141
9.3	Laws of war	144
9.4	Key issues	151
 Part III: Country Perspectives		
10	RMA: The Russian Way	157
	<i>Fanourios Pantelogiannis</i>	
10.1	Historical overview	157
10.2	The current Russian RMA and its international consequences	159
10.3	Conclusion and evaluation	166
10.4	Perspectives	167
11	An Overview of the Research and Development of Information Warfare in China	173
	<i>Chris Wu</i>	
11.1	Introduction	173
11.2	Theoretical research on Information Warfare in China	174
11.3	Current IW development in China	182
11.4	IW tactics that could be used by Beijing to attack Taiwan	189
11.5	Combination of US and Taiwanese resistance to IW from Beijing	191

11.6	The possibility of IW between China and the USA	191
11.7	Conclusion	193

Part IV: What is Being Done – or Must Be Done?

12	A Bridge Too Far?	199
	<i>Mike Moore</i>	
12.1	Global engagement	201
12.2	A space Pearl Harbor?	204
12.3	Space cop	206
12.4	The security dilemma	208
12.5	A mind experiment	210
12.6	Velvet glove, steel fist	212
12.7	Unintended consequences	213
12.8	'Last, best hope'	216
13	Threat Assessment and Protective Measures: Extending the Asia–Europe Meeting IV Conclusions on Fighting International Terrorism and Other Instruments to Cyber Terrorism	219
	<i>Massimo Mauro</i>	
13.1	Introduction	219
13.2	The Asia–Europe Meeting (ASEM) framework	219
13.3	Cyber terrorism: an urban legend?	220
13.4	A taxonomy of real cyber threats	222
13.5	Advanced defensive methods and different regional priorities	224
13.6	International and regional cooperation against cyber terrorism	224
13.7	Concluding statement	225
14	Policy Laundering, and Other Policy Dynamics	228
	<i>Dr Gus Hosein</i>	
14.1	Introduction	228
14.2	At the international level: the Council of Europe and the G8	230
14.3	At the national level	232
14.4	The international–national dance: traffic data retention	234
14.5	Democratic challenges and international opportunities	236
14.6	Concluding remarks	239

15 Conclusion	242
<i>Dr Steve Wright, Dr Philippa Trevorrow, Professor David Webb and Dr Edward Halpin</i>	
<i>Index</i>	246