

CONTENTS

<i>List of Contributors</i>	<i>page</i>	viii
<i>Acknowledgements</i>		xiii
<i>List of Abbreviations</i>		xiv
1	Introduction	1
TOMOKO ISHIKAWA AND YARIK KRYVOI		
1.1	Background: Cybersecurity and the Backlash against Economic Globalisation	1
1.2	Aims and Scope	3
1.3	Overview of the Chapters	8
2	International Relations Perspectives: Cybergovernance in the Post-liberal Order	12
KIICHI FUJIWARA AND PAUL NADEAU		
2.1	Introduction	12
2.2	Creating a Governance Regime for Borderless Threats	14
2.3	Actors and Stakeholders	27
2.4	Conclusion	35
3	The State-Oriented Model of Internet Regulation: The Case of China	40
WAKAKO ITO		
3.1	Introduction	40
3.2	Views on Internet Regulation under the Xi Administration	41
3.3	The Framework of Internet Regulation in China	50
3.4	China's Approach to International Cybergovernance	59
3.5	Conclusion	66
4	Cybercrime, the United Nations, Prospects, and Challenges for International Co-operation	69
SUMMER WALKER AND IAN TENNANT		
4.1	Introduction	69

4.2	Broader International Law Relevance	71
4.3	Cybercrime at the UN: A Historical Background	74
4.4	The Underlying Debates That Limit Global Agreement	78
4.5	2019–2022 Negotiations: The Politics of Modalities	87
4.6	Is There Shared Purpose? States Diverge on Scope of Crimes, but Move Closer Together on Procedural Measures: May–June 2022	94
4.7	Conclusion	102
5	Responding to Public and Private Cyberattacks: Jurisdiction, Self-Defence, and Countermeasures	103
	YARIK KRYVOI	
5.1	Introduction	103
5.2	Conceptual Framework	104
5.3	The Nature and Legal Regimes of Private and Public Cyberattacks	104
5.4	Responding to Cyberattacks	117
5.5	Conclusion	131
6	International Data Transfers and Cybersecurity: Three Regulatory Approaches and Their Implications	134
	JENS HILLEBRAND POHL	
6.1	Introduction	134
6.2	The Cybersecurity Aspect of International Data Transfers	136
6.3	Effectiveness of Data-Transfer Regulation as a Cybersecurity- Policy Instrument	156
6.4	Conclusion	159
7	International Trade Law and Cybersecurity: Balancing Free Markets and Regulation	161
	ELIZABETH WHITSITT	
7.1	Introduction	161
7.2	The Shifting Interface between International Trade Law and Cybersecurity: From Multilateralism to Regionalism	165
7.3	Regulating Cybersecurity as a Security Exception	168
7.4	Regulating Cybersecurity under Electronic Commerce (and Other) RTA Provisions	178
7.5	Concluding Remarks	183

8 Cyberthreats, Human Rights, and FDI Restrictions 185**TOMOKO ISHIKAWA**

- 8.1 Introduction 185
- 8.2 The Impact of Cyber Actions on Human Rights 186
- 8.3 States' Duty to Protect 189
- 8.4 Global Trend to Tighten FDI Restrictions 195
- 8.5 Possible Investment Claims Arising from FDI Restrictions 198
- 8.6 The Application of a Security-Based Defence for Cybersecurity Measures: The Dilemma 200
- 8.7 Conclusion: Need for a Mechanism for Co-operation 209

9 Public–Private Partnerships on Cybersecurity and International Law: Finding Multilateral Solutions 211**ALEKSANDER KALISZ**

- 9.1 Introduction 211
- 9.2 Public–Private Consensus on Expanding Cybersecurity PPPs 214
- 9.3 PPPs in Domestic Laws: Finding Common Ground 222
- 9.4 Models for the International Harmonisation of Cybersecurity PPPs 227
- 9.5 Conclusions 237

10 The Geopolitical Divide, Norm Conflict, and Public–Private Partnership in Cybersecurity Governance 240**YARIK KRYVOI AND TOMOKO ISHIKAWA**

- 10.1 Introduction 240
- 10.2 The Nature of Cybersecurity Governance 242
- 10.3 States Willing to Co-operate on Cybersecurity Matters 244
- 10.4 Limits to Co-operation on Cybersecurity Governance 245
- 10.5 Existing Regional Agreements That Reflect Market-Oriented and State-Oriented Models 250
- 10.6 Regional Co-operation as a Realistic Way Forward for Cybersecurity Co-operation and the Potential for Broader Co-operation 255
- 10.7 Role of the Private Sector in Cybersecurity Governance 257
- 10.8 Future Outlook 263

***Index* 265**