

Contents

	<i>List of Figures</i>	<i>page</i>	viii
	<i>Preface</i>		ix
	<i>Acknowledgments</i>		xvi
	<i>List of Abbreviations</i>		xix
PART I OF BROKERS AND PROXIES			
1	Cyber Proxies: An Introduction		3
	Proxies and Cyber Power		6
	What Cyber Proxies Are (Theoretically) Capable Of		8
	What Cyber Proxies Are Likely to Be Used For		14
	The Pool of Potential Cyber Proxies		16
	Proxy Relationships and Selected Cases		20
	Proxies and the Attribution Problem		22
	A Few Words on Methodology		25
	Conclusion: Cyber Proxies and the Bigger Picture		26
2	Proxies: An Instrument of Power Since Ancient Times		29
	Framework for Thinking About Proxies		31
	Why Proxy Relationships Exist		35
	Three Main Types of Proxy Relationships: Delegation, Orchestration, and Sanctioning		42
	Conclusion: It's the Relationship That Matters		48
3	Cyber Power: Geopolitics and Human Rights		50
	The Bigger Picture: Sovereignty and Information		52
	The US Government's Perspective		55
	The Russian Government's Perspective		58
	The Chinese Government's Perspective		61

	The Iranian Government's Perspective	64
	Conclusion: Cybersecurity Is in the Eye of the Beholder	66
	PART II CYBER PROXIES UP CLOSE	69
4	Cyber Proxies on a Tight Leash: The United States	71
	Private Cybersecurity Contractors	73
	Delegation Under the Spotlight: US Cyber Command and Cybersecurity Contractors	76
	Private Cybersecurity Contractors and Internal Security	78
	Conclusion: Predictable Proliferation of Capabilities	79
5	Cyber Proxies on a Loose Leash: Iran and Syria	81
	Orchestration Under the Spotlight: The US Indictment of Iranian Hackers	84
	Orchestration in Wartime: The Syrian Electronic Army	89
	Conclusion: Unexpected Escalation and Limited Options for Response	92
6	Cyber Proxies on the Loose: The Former Soviet Union	94
	Sanctioning in Peacetime: The 2007 DDoS Attack on Estonia	97
	Sanctioning in Wartime: The Conflict in Ukraine (2014–Today)	98
	Blitz Orchestration: The War Against Georgia in 2008	101
	Sanctioning and Mobilizing: The March 2017 US Indictment of Russian Hackers	103
	Conclusion: Sanctioning and Statehood	105
7	Change Over Time: China's Evolving Relationships with Cyber Proxies	107
	The Rise of Hacktivists in China and the Government's Passive Support (1994–2003)	108
	The Creation of Militia Units and the Move Towards Orchestration (2003–13)	112
	Tightening Control and Aspirational Delegation (2013–Today)	115
	Conclusion: From Broker State to (Aspirational) Monopolist	117
	PART III IMPLICATIONS	121
8	The Theory: State Responsibility and Cyber Proxies	123
	A Framework for Cyber Proxy Relationships Based on International Law	125
	Due Diligence	130

Third Countries and Extraterritoriality	132
Conclusion: International Cooperation Under Pressure	134
9 The Practice: Shaping Cyber Proxy Relationships	138
Keeping One's Own House in Order: Determining Inherently Governmental Functions	142
Keeping One's Own House in Order: Determining the Role of the Private Sector	144
Keeping One's Own House in Order: Nationalism and Hacktivism	146
Conclusion: Nudging and Managing Instead of Dictating and Prohibiting	149
10 Conclusion: Cyber Proxies, the Future, and Suggestions for Further Research	151
<i>Future Research</i>	158
<i>Notes</i>	164
<i>Index</i>	235