

Contents

<i>Preface</i>	vii
<i>Acknowledgments</i>	ix

Introduction	1
--------------	---

PART I CYBERATTACKS AND RESTRAINT

1. Defining and Studying Cyberattacks	11
1.1 Estonia Was a Rehearsal	11
1.2 Topic and Scope	14
1.3 Defining Cyberattacks	19
1.4 Assumptions and Present Realities	40
2. Defining and Studying Restraint	53
2.1 Framing the Analysis	54
2.2 Concepts and Methodologies	55
2.3 Evolution of the Literature	66
2.4 Critiquing Restraint	78
2.5 Overview of Book	84

PART II DETERRENCE

3. Evaluating Deterrence	87
3.1 Defining Rationalist Deterrence	90
3.2 Cyberattack Capabilities as a Deterrent	102
3.3 Alternative Deterrence Frames	121
3.4 Moving Beyond Cyber-Deterrence	125
4. Constructing Deterrence	127
4.1 Defining Structural Deterrence	128
4.2 Evidence of Structural Deterrence	133
4.3 Whose Deterrence Succeeds?	150
Conclusions	152

PART III INTERNATIONAL LAW AND THE USE OF FORCE

5. Limiting the Use of Force	157
5.1 Locating Relevant Law	159
5.2 Cyberattacks as an Article 2(4) Use of Force	167
5.3 Cyberattacks as Violations of Integrity, Independence, or Purposes	182
Conclusions	197
6. Constructing Self-Defense	200
6.1 Applying the Remedial <i>Jus ad Bellum</i>	202
6.2 Cyberattacks and the Remedial <i>Jus Ad Bellum</i>	209
6.3 Structural Remediation	227
Conclusions	236

PART IV HUMANITARIAN PROTECTIONS

7. Humanitarian Protections	239
7.1 Approaching Humanitarian Protections	242
7.2 Indiscriminateness	253
7.3 Injury to Protected Classes	266
7.4 Disproportionality	281
Conclusions	286
8. Constructing a Prohibition	289
8.1 Moving Beyond Cyber Arms Control	291
8.2 Structural Prohibition	294
8.3 Understanding Prohibitive Norms	301
8.4 Cyberattack Norm Construction	306
8.5 Cyberattack Norm Evolution	322
Conclusions	333
Conclusion	335
<i>Bibliography</i>	343
<i>Index</i>	387