

## Contents

<i>Preface</i>	<i>page</i>	ix
<i>Acknowledgements</i>		xi
<b>PART I CYBERSECURITY INCIDENTS AND INTERNATIONAL LAW</b>		<b>1</b>
<b>1 The Spectre of Cyberwar</b>		<b>3</b>
<b>2 Terminology</b>		<b>17</b>
<b>3 International Legal Framework</b>		<b>21</b>
3.1 Cybersecurity Incidents and the Prohibition on the Use of Force		21
3.2 Cybersecurity Incidents and the Principle of Non-intervention		32
3.3 Cybersecurity Incidents and Violations of Sovereignty		38
3.4 Conclusion		41
<b>PART II UNILATERAL REMEDIES TO CYBERSECURITY INCIDENTS</b>		<b>43</b>
<b>4 Self-Defence</b>		<b>47</b>
4.1 Preconditions of Self-Defence		47
4.2 Cybersecurity Incidents as Armed Attacks		56
4.3 Preliminary Conclusion		64
4.4 The Attribution Problem		65
4.5 The Time Factor		109
4.6 Conclusion		112

5	<b>Countermeasures</b>	113
5.1	Preconditions of Countermeasures	113
5.2	Countermeasures as a Remedy for Cybersecurity Incidents	123
5.3	Countermeasures for Other Purposes	179
5.4	Conclusion	200
6	<b>Necessity</b>	201
6.1	Necessity in Customary International Law	204
6.2	Preconditions of Necessity	207
6.3	Necessity and the Question of the Use of Force	229
6.4	Legal Consequences	251
6.5	Conclusion	255
PART III OUTLINES OF AN EMERGENCY REGIME FOR CYBERSPACE		259
7	<b>Transnational Cybersecurity, Unilateral Remedies, and the Rule of Law</b>	261
8	<b>‘Such Incidents Might Recur at Any Time’: The Intervention Convention</b>	267
9	<b>Possible Elements of the Cyber Emergency Regime</b>	272
9.1	Preconditions for Protective Conduct	272
9.2	<i>Ex Post Facto</i> Assessment	274
9.3	Accountability for Vulnerabilities Retention	279
10	<b>Concluding Remarks</b>	282
	<i>Bibliography</i>	285
	<i>Index</i>	319