Contents

Table of Cases xv
Table of Legislation and Other Documents xix
List of Abbreviations xxvii

1. Identifying the Problem and the Applicable Law 1
I. The Emergence of the Cyber Threat to International Security 1
II. The Taxonomy of Military Cyber Operations: Definitions and Classification 10
III. The Applicable Law: *Inter (Cyber) Arma Enim Silent Leges*? 19
IV. Identification and Attribution Problems 33
V. The Book's Scope and Purpose 40

2. Cyber Operations and the *jus ad bellum* 43
I. Introduction 43
II. Cyber Operations and the Prohibition of the Threat and Use of Force in International Relations 44
III. Cyber Operations and the Law of Self-Defence 69
IV. Remedies Against Cyber Operations Short of Armed Attack 104
V. Chapter VII of the United Nations Charter and the Role of the Security Council 110
VI. Conclusions 115

3. The Applicability of the *jus in bello* to Cyber Operations 117
I. Introduction 117
II. Cyber Operations in and as International Armed Conflicts 119
III. Cyber Operations During Partial or Total Belligerent Occupation 141
IV. Cyber Operations in and as Non-International Armed Conflicts 148
V. Cyber Operations as 'Internal Disturbances and Tensions' 159
VI. Conclusions 161

4. Cyber Operations and the Conduct of Hostilities 164
I. Introduction 164
II. The Legality of Means and Methods of Cyber Warfare 168
III. The Law of Targeting 176
IV. Cyber Operations Short of 'Attack' 239
V. Cyber Operations as Remedies Against Violations of the Law of Armed Conflict 242
VI. Conclusions 245

5. Cyber Operations and the Law of Neutrality 246

I. Introduction 246
II. When Does the Law of Neutrality Apply? 248
III. The Law of Neutrality and its Consequences on the Conduct of Cyber Operations 253
IV. Non-Belligerency 267
V. The Law of Neutrality and the UN Charter 269
VI. Remedies Against the Violations of the Law of Neutrality 272
VII. Conclusions 277

General Conclusions 280

Select Bibliography 289
Index 301