Contents

Acknowledgements page xi
Table of cases xiii
List of abbreviations xvi

1 The world in which we live and fight **1**
1 Computer network attacks 4
2 Law and war in the internet age 8
3 Societal trends generally 11
3.1 The information revolution and digitisation 11
3.2 Globalisation, interdependency and the changing world order 17
3.3 The rise of the knowledge economy 20
4 Military trends 21
4.1 A change of purpose 23
4.2 Network-centric warfare and effects-based operations 24
4.3 Outsourcing and civilianisation 25
5 Terminology and definitions 27
5.1 New laws for old? 28
5.2 Methodology 30
5.3 A word about examples and hypotheticals 31
6 Conclusion 32

PART I Jus ad bellum

2 Computer network attacks as a use of force in international law **37**
1 Force defined as armed force 40
2 Definition of armed force 49

2.1 State actions 53

2.2 Theories of force – scholastic writings 58

3 Computer network attacks as a use of force 62

3.1 Characteristics of computer network attacks 65

4 Conclusion 74

3 Armed attack and response in the digital age 75

1 Armed attack 76

1.1 Anticipatory self-defence 82

1.2 Pinprick attacks or accumulation of events theory 93

2 Self-defence against non-state actors 95

3 Attribution 99

4 Necessity and proportionality 102

5 Countermeasures against unlawful acts 105

6 Security Council authorisation and collective measures 109

7 Conclusion 113

PART II Jus in bello

4 The applicability of the laws of armed conflict to computer network attacks 117

1 Armed conflict 118

1.1 The requirement of armed force 122

1.2 Intervention of the armed forces 123

2 Application to computer network attacks 126

2.1 Application during conventional armed conflict 127

2.2 Computer network attack on its own 129

2.3 Computer network attacks in support of conventional attacks 134

3 Territory 134

4 Conclusion 137

5 Participants in conflict: combatant status, direct participation and computer network attack 139

1 Combatant status 140

1.1 Requirements of combatant status 144

1.2 Saboteurs and spies 151

2 Direct participation by civilians 159

2.1 Requirements of direct participation 161

2.2 Offensive computer network attack 167

2.3 Computer network attack system support 167

2.4 Generic IT support 170

2.5 Mercenaries 172
3 Child soldiers 175
4 Conclusion 178

6 Targeting and precautions in attack 179
1 The principle of distinction 180
2 Legitimate military objectives 184
2.1 Nature, location, purpose or use 185
2.2 Effective contribution to military action 188
2.3 Definite military advantage 190
3 Dual-use technology 193
4 Protection of civilian objects 195
4.1 Attacks and operations 196
4.2 Indiscriminate attacks 202
5 Proportionality 205
5.1 Knock-on effects 207
5.2 Dual-use systems 208
6 Precautions in attack 209
6.1 Verification of military objectives 211
6.2 Choice of weapons 212
6.3 Choice of targets 216
7 Precautions against the effects of attacks 217

7 Measures of special protection 220
1 The environment 221
1.1 Additional Protocol I 222
1.2 ENMOD Convention 224
1.3 Other protections 226
2 Cultural property 227
2.1 The legal framework 228
2.2 Attacks on, and damage to, digital works 233
2.3 Theft, pillage or misappropriation of digital works 235
3 Installations containing dangerous forces 239
4 Objects indispensable to the survival of the civilian population 243
5 Hospitals and other medical units 244
5.1 Location and access to medical databases 244
5.2 Hospital ships 247
6 Non-defended localities and demilitarised zones 247
6.1 Non-defended localities 248
6.2 Demilitarised zones 248

8 Means and methods of warfare **250**

1 Law of weaponry 251

1.1 General principles 252

1.2 Explicit prohibitions of weapons 258

1.3 Article 36 obligations 260

2 Perfidy and ruses of war 261

2.1 Ruses of war 261

2.2 Perfidy 263

2.3 Misuse of protected symbols and emblems 264

3 Destruction and seizure of property 265

3.1 Booty 270

3.2 Occupied territory 272

3.3 Pillage and plunder 274

3.4 Enemy-owned property on the territory of a belligerent 276

4 Conclusion 277

Concluding remarks **279**

Appendix 1 Selected computer network attack examples 281

Appendix 2 Glossary of selected computing terms 293

Bibliography 297

Index 321