

# Contents

<b>1 Introduction: Perspectives of Various Stakeholders and Challenges for International Law</b> .....	1
1.1 Perspectives of Stakeholders.....	1
1.2 General Introduction to Public International Law .....	15
1.3 Food for Thought.....	21
<b>2 Jurisdiction and Attribution of State Responsibility in Cyberspace</b> .....	23
2.1 Jurisdiction.....	23
2.2 Attribution of State Responsibility .....	32
2.2.1 ILC's Draft Articles on State Responsibility.....	36
2.2.2 Standard(s) of Proof .....	40
2.2.3 Attribution and International Organizations, Such As NATO .....	43
<b>3 Regulation of Cyberspace and Human Rights</b> .....	45
3.1 General Background .....	45
3.2 Human Rights in Cyberspace .....	53
3.2.1 Privacy and Related Rights .....	54
3.2.2 Right to the Freedom of Expression.....	84
3.2.3 Anonymity and the Right to Be Forgotten .....	87
3.3 Exceptions.....	94
3.3.1 European Practice.....	101
3.3.2 US Practice.....	111
3.3.3 Some Examples of Practice in Other Global Regions.....	128
3.4 Territorial Scope of Human Rights Protection and Extraterritorial Jurisdiction Regarding Search Warrants and Other Law Enforcement Measures .....	132
3.5 Food for Thought.....	150

<b>4</b>	<b>Cyber Warfare</b> .....	153
4.1	Cyberattack.....	153
4.2	Cyber Warfare.....	158
4.3	Cyber Weapons.....	160
4.4	Use of Force Under International Law.....	161
4.5	Armed Attack and the Right of Self-Defence.....	166
4.6	Self-Defence Against Non-State Actors.....	175
4.7	Countermeasures.....	191
4.8	Necessity.....	192
4.9	Reprisals.....	193
4.10	Retorsion.....	194
4.11	Neutrality in Cyberspace.....	195
4.12	Cyber Disarmament.....	196
<b>5</b>	<b>Application of the Law of Armed Conflict, Including International Humanitarian Law, In Cyberspace</b> .....	201
5.1	The Law of Armed Conflict/International Humanitarian Law.....	202
5.2	International Armed Conflict.....	208
5.3	Non-international Armed Conflict.....	224
5.4	War Crime of Terrorism.....	228
5.5	Food for Thought.....	229
<b>6</b>	<b>Cyber Espionage</b> .....	233
6.1	Modus Operandi.....	234
6.2	Targets.....	236
6.3	International Law on Espionage.....	241
6.4	Food for Thought.....	260
<b>7</b>	<b>Cyber Crimes</b> .....	263
7.1	Cyber Crimes: The Challenges.....	263
7.2	Budapest Convention: Model for Universal Suppression of Cyber Crimes.....	270
7.3	Beyond the Budapest Convention.....	292
<b>8</b>	<b>Cyber Terrorism</b> .....	295
8.1	Acts of Terrorism Against Civil Aviation.....	299
8.2	Acts of Terrorism Against Potential Victims.....	308
8.3	Acts of Terrorism at Sea.....	310
8.4	Acts of Terrorism Relating to Dangerous Materials.....	313
8.5	Terrorist Financing.....	318
8.6	Developments Beyond the Sectoral Conventions.....	322
8.7	National Laws.....	324

<b>9 Future Prospects of Public International Law of Cyberspace.....</b>	<b>335</b>
9.1 Stocktaking.....	335
9.2 Cybersecurity.....	343
9.3 Cyber Deterrence.....	343
9.4 Cyberspace Governance .....	347
9.5 Cyber Sovereignty .....	352
<b>Glossary .....</b>	<b>357</b>
<b>Bibliography .....</b>	<b>359</b>