

# CONTENTS

*Acknowledgements* ..... vii  
*Abbreviations* ..... xv

**Introduction** ..... 1

1. Research Question ..... 1
2. Objectives of the Study ..... 3
3. Research Subject ..... 4
4. Structure of the Study ..... 5

## PART I. THE INTERNET AS A UNIVERSAL YET TERRITORIALISED INFRASTRUCTURE

**Chapter 1. A Survey of Computer Network Operations** ..... 9

1. The Medium of Computer Network Operations: the Internet ..... 9
  - 1.1. The Internet as a Network of Networks: Technical Fundamentals ... 9
  - 1.2. The Significance of the Internet for Modern Societies ..... 13
    - 1.2.1. The Information and Knowledge Society ..... 13
    - 1.2.2. State and eGovernment ..... 17
    - 1.2.3. The Military Sector ..... 18
2. The Characteristics of Computer Network Operations ..... 20
  - 2.1. Defining and Differentiating Computer Network Operations ..... 20
    - 2.1.1. In Military Doctrine ..... 21
    - 2.1.2. In Legal Scholarship ..... 23
    - 2.1.3. Approach of this Study ..... 24
  - 2.2. The Technicalities of Computer Network Operations ..... 25
    - 2.2.1. The Main Types of Malicious Computer Network Operations ..... 26
      - 2.2.1.1. Distributed Denial of Service Attacks ..... 26
      - 2.2.1.2. Trojan Horses, Computer Viruses and Worms ..... 27
    - 2.2.2. Tracing Computer Network Operations back to their Source ..... 28
  - 2.3. Target Scenarios of Computer Network Operations ..... 31
    - 2.3.1. Military Targets ..... 31
    - 2.3.2. The Public Infrastructure as a Target ..... 33
    - 2.3.3. Interference with Financial Assets ..... 36
  - 2.4. Conclusion ..... 37

3. Case Studies .....	38
3.1. Computer Network Espionage .....	39
3.2. Estonia 2007 .....	42
3.3. Georgia 2008 .....	45
3.4. Stuxnet and the Iranian Nuclear Programme .....	47
3.5. Conclusion .....	50

**Chapter 2. The Legal Regime of Cyberspace .....** 53

1. Jurisdiction in Cyberspace .....	53
1.1. Cyberspace as a Jurisdiction Sui Generis .....	53
1.2. Cyberspace as an International Commons .....	55
1.3. The Territorialisation of Cyberspace .....	58
1.3.1. Jurisdiction to Prescribe .....	59
1.3.2. Jurisdiction to Adjudicate .....	60
2. Actors in Cyberspace .....	62
2.1. International Internet Regulation .....	62
2.1.1. Internet Governance .....	62
2.1.2. Technical Regulation .....	66
2.1.3. Content Regulation .....	67
2.2. Internet Security Organisations .....	67
2.3. The Militarisation of Cyberspace .....	71
2.3.1. Within the United States Military .....	71
2.3.2. Within Other Militaries .....	73
3. The Gradual Development of Common Cybersecurity Standards .....	76
3.1. The International Level .....	76
3.2. The Regional Level .....	77
4. Conclusion: the Territorialisation of a Universal Infrastructure .....	79

**PART II. THE LEGAL QUALIFICATION OF COMPUTER NETWORK OPERATIONS**

**Chapter 3. Computer Network Operations Outside of Armed Conflict .....** 85

1. Rules of Attribution .....	87
1.1. Actions of States .....	88
1.1.1. Actions of States through their Organs .....	88
1.1.2. Actions of States through Non-State Actors .....	89
1.1.2.1. The Required Level of Control .....	89
1.1.2.2. The Level of Control over Computer Network Operations .....	91
1.2. Omissions of State Organs .....	94
1.2.1. The General Criteria of the Duty to Exercise Due Diligence .....	96
1.2.1.1. No Justification by Recourse to National Law .....	96

1.2.1.2.	The Element of Disposability of Means . . . . .	97
1.2.1.3.	Prosecution of Individual Perpetrators und National Criminal Laws . . . . .	98
1.2.1.4.	The Principle of Proportionality . . . . .	99
1.2.2.	Due Diligence and Malicious Computer Network Operations . . . . .	99
1.2.2.1.	The Thesis of a Specific Obligation . . . . .	100
1.2.2.2.	A General Obligation to Prevent Malicious Cross-Border Computer Network Operations . . . . .	102
2.	Breach of an International Obligation . . . . .	111
2.1.	Computer Network Operations Below the Level of Armed Force . .	111
2.1.1.	The Prohibition of Intervention . . . . .	112
2.1.1.1.	Domaine Réservé in Cyberspace . . . . .	113
2.1.1.2.	Means of Interference . . . . .	116
2.1.1.3.	Conclusion . . . . .	127
2.1.2.	The Regime of International Telecommunications . . . . .	127
2.1.3.	The Regime of Outer Space . . . . .	131
2.1.4.	The Law of the Sea . . . . .	133
2.1.5.	Conclusion . . . . .	134
2.2.	The Prohibition of the Use of Forceful Computer Network Operations . . . . .	135
2.2.1.	The Notion of Force . . . . .	135
2.2.1.1.	Armed Force and Economic Coercion . . . . .	136
2.2.1.2.	Physical Force . . . . .	138
2.2.2.	Computer Network Operations as Armed Force . . . . .	140
2.2.2.1.	The Applicability Ratione Loci of the UN Charter in Cyberspace . . . . .	140
2.2.2.2.	The Different Approaches of Qualifying Computer Network Operations as Force . . . . .	141
3.	Circumstances Precluding Wrongfulness . . . . .	155
3.1.	Force Majeure . . . . .	155
3.2.	Computer Network Operations as Countermeasures . . . . .	157
3.2.1.	The Absence of a Self-Contained Regime Applicable to Computer Network Operations . . . . .	157
3.2.2.	Subsidiarity of Countermeasures . . . . .	158
3.2.3.	Possible Computer Network Operation Countermeasures . . . . .	159
3.2.3.1.	Automated Responses . . . . .	159
3.2.3.2.	A Right of ‘Cyber Hot Pursuit’? . . . . .	162
3.2.3.3.	Human Rights as Limits to Countermeasures . . . . .	163
4.	Conclusion . . . . .	173

<b>Chapter 4. The Justified Use of Forceful Computer Network Operations . . .</b>	<b>175</b>
1. The Right of Self-Defence . . . . .	175
1.1. Requirements for the Presumption of an Armed Attack . . . . .	176
1.1.1. General Requirements . . . . .	176
1.1.2. Computer Network Operations as an Armed Attack . . . . .	178
1.1.3. The Gathering of Evidence in Proof of a Claim to Act in Self-Defence . . . . .	181
1.2. Self-Defence against Non-State Actors . . . . .	183
1.3. Anticipatory and Pre-emptive Self-Defence . . . . .	188
1.4. Limits to the Right of Self-Defence . . . . .	191
2. UN Security Council Enforcement Measures . . . . .	192
2.1. The Prerequisites for a Decision of the UN Security Council . . . . .	192
2.2. Computer Network Operations as Measures under Chapter VII . . .	194
3. Conclusion . . . . .	196
<b>Chapter 5. Computer Network Operations During an International Armed Conflict . . . . .</b>	<b>197</b>
1. Introduction . . . . .	197
2. The Applicability of International Humanitarian Law to Military Computer Network Operations . . . . .	200
2.1. General Applicability of Humanitarian Law to New Weapons . . . .	200
2.2. The Spatial Applicability of Humanitarian Law: the Region of War . . . . .	204
2.3. The Qualification of Military Computer Network Operations as an Attack under International Humanitarian Law . . . . .	205
3. The Rules of Humanitarian Law as Applied to Military Computer Network Attacks . . . . .	208
3.1. The Rules concerning the Methods of Computer Network Attacks . . . . .	208
3.1.1. Precautions before Launching Computer Network Attacks . . . . .	210
3.1.2. The Principle of Distinction . . . . .	213
3.1.2.1. The Prohibition of Indiscriminate Attacks . . . . .	214
3.1.2.2. The Wearing of Uniform . . . . .	216
3.1.2.3. The Duty to Separate Military from Civilian Targets . . . . .	217
3.1.3. Perfidy and Ruses in Cyber Warfare . . . . .	221
3.1.4. The Principle of Proportionality in Cyber Warfare . . . . .	226
3.2. Valid Targets of Computer Network Attacks, Their Control and Abandonment . . . . .	228
3.2.1. The Military Objectives of Cyber Warfare . . . . .	228
3.2.2. Controlling Military Objectives via Cyber Warfare . . . . .	232

3.2.3. The Clearance of Remnants Caused by Cyber Warfare. . . . .	233
3.3. The Status of Actors in Cyber Warfare . . . . .	236
3.3.1. Combatants in Cyber Warfare. . . . .	236
3.3.1.1. Regular Members of Armed Forces. . . . .	236
3.3.1.2. The Utilisation of Individuals who are not Regular Members of the Armed Forces of a State. . . . .	237
3.3.2. Civilian Participation in Cyber Warfare . . . . .	242
3.3.2.1. Actions Taken in Cooperation with the Armed Forces . . . . .	244
3.3.2.2. Actions by Civilians Taken Independently from the Armed Forces . . . . .	247
3.3.2.3. Cyber Levée en Masse . . . . .	248
3.3.3. Spies and Computer Network Espionage. . . . .	251
4. Limits: Human Rights . . . . .	254
5. Conclusion . . . . .	256
<b>Chapter 6. Neutrality in Cyber Warfare . . . . .</b>	<b>259</b>
1. No Prohibition on Routing CNAs through Neutral States' Territory. . . . .	260
2. The Prohibition on Masking CNAs as Originating from a Neutral State . . . . .	264
3. Obligations of Neutral States. . . . .	265
4. The Hosting of Government Websites on Foreign Servers. . . . .	267
5. Conclusion . . . . .	270
<b>PART III. CONCLUSION</b>	
<b>Computer Network Operations Restrained. . . . .</b>	<b>273</b>
<i>Bibliography . . . . .</i>	<i>279</i>