CYBER WARFARE
CYBER WARFARE

Military Cross-Border Computer Network Operations under International Law

Johann-Christoph Woltrog

intersentia
Cambridge - Antwerp - Portland
Cyber Warfare. Military Cross-Border Computer Network Operations under International Law
Johann-Christoph Woltag

© 2014 Intersentia
Cambridge – Antwerp – Portland
www.intersentia.com | www.intersentia.co.uk

D/2014/7849/59
NUR 828


No part of this book may be reproduced in any form, by print, photoprint, microfilm or any other means, without written permission from the publisher.
To my parents
ACKNOWLEDGEMENTS

This book was largely written during my time as a research fellow at the Max Planck Institute for Comparative Public Law and International Law in Heidelberg and was accepted as a doctoral thesis at the University of Hamburg in 2013. I am especially grateful for the academic supervision of my doctoral supervisor Professor Dr. Dr. h.c. Rüdiger Wolfrum who gave me the necessary freedom in the writing of this book. I would also like to extend my appreciation to Professor Dr. Markus Kotzur, LL.M., who served as my second reader.

Ann-Christin Maak-Scherpe and Rebecca Pound of Intersentia deserve thanks for their guidance and support in the publication process and Professor Dr. Jan Wouters for agreeing to publish the study in the International Law series.

I would like to thank everyone at the Max Planck Institute for all of their support, especially my friends and colleagues who, in a variety of different ways, supported me during this time. Deserving of special mention are Dominik Zimmermann, LL.M., Florian Wenk, LL.M., Dr. Clemens Feinäugle, Sigrid Mehring, LL.M., Dr. Daniel Heilmann, LL.M., Dr. Marc Jacob, LL.M., Hans Christian Wilms, Dr. Stephan Schill, LL.M. and Daniela Arrese, LL.M.

I am particularly grateful for the invaluable support of John Henry Dingfelder Stone, LL.M. My personal thanks go to Dr. Isabel Röcker, who read the manuscript and strongly encouraged me throughout the entire writing process.

I dedicate this book to my parents, Dorothee and Helmut Woltag, who accompanied me through the sometimes strenuous undertaking of my doctoral studies in law.

Heidelberg, January 2014

Johann-Christoph Woltag
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
3.2.2. 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
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

Chapter 6. Neutrality in Cyber Warfare ............................... 259
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

PART III. CONCLUSION

Computer Network Operations Restrained ............................ 273

Bibliography ............................................................... 279
# ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banjul Charter</td>
<td>African Charter on Human and Peoples’ Rights</td>
</tr>
<tr>
<td>ACHR</td>
<td>American Convention on Human Rights</td>
</tr>
<tr>
<td>Genocide Convention Case</td>
<td>Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Judgment)</td>
</tr>
<tr>
<td>UN Charter</td>
<td>Charter of the United Nations</td>
</tr>
<tr>
<td>CNA</td>
<td>Computer Network Attack</td>
</tr>
<tr>
<td>CNO</td>
<td>Computer Network Operation</td>
</tr>
<tr>
<td>Hague Regulations of 1907</td>
<td>Convention concerning the Laws and Customs of War on Land and its Annex: Regulations Respecting the Laws and Customs of War on Land</td>
</tr>
<tr>
<td>Hague Convention V</td>
<td>Convention respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land</td>
</tr>
<tr>
<td>CCDCOE</td>
<td>Cooperative Cyber Defence Centre of Excellence</td>
</tr>
<tr>
<td>COE</td>
<td>Council of Europe</td>
</tr>
<tr>
<td>ccTLD</td>
<td>Countrycode Top-Level Domain</td>
</tr>
<tr>
<td>CIP</td>
<td>Critical Infrastructures Protection</td>
</tr>
<tr>
<td>St. Petersburg Declaration</td>
<td>Declaration Renouncing the Use in Time of War of Explosive Projectiles under 400 Grammes Weight</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights</td>
</tr>
<tr>
<td>ECtHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>ENISA</td>
<td>European Network and Information Security Agency</td>
</tr>
<tr>
<td>fn.</td>
<td>Footnote</td>
</tr>
<tr>
<td>Geneva Convention III</td>
<td>Geneva Convention relative to the Treatment of Prisoners of War</td>
</tr>
<tr>
<td>Abbreviations</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Manual on Air and Missile Warfare</td>
<td>Humanitarian Policy and Conflict Research</td>
</tr>
<tr>
<td>ILC Articles on State Responsibility</td>
<td>ILC Articles on Responsibility of States for Internationally Wrongful Acts</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>ICCPR</td>
<td>International Covenant on Civil and Political Rights</td>
</tr>
<tr>
<td>ICRC</td>
<td>International Committee of the Red Cross</td>
</tr>
<tr>
<td>ICTY</td>
<td>International Criminal Tribunal for the Former Yugoslavia</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>ICANN</td>
<td>Internet Corporation for Assigned Names and Numbers</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>Israeli Wall Advisory Opinion</td>
<td>Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion)</td>
</tr>
<tr>
<td>MPEPIL</td>
<td>Max Planck Encyclopedia of Public International Law</td>
</tr>
<tr>
<td>Joint Project Agreement</td>
<td>Memorandum of Understanding between the US Department of Commerce and ICANN</td>
</tr>
<tr>
<td>Nicaragua Case</td>
<td>Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits)</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>Additional Protocol I</td>
<td>Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts</td>
</tr>
<tr>
<td>Additional Protocol II</td>
<td>Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts</td>
</tr>
<tr>
<td>RIAA</td>
<td>Reports of International Arbitral Awards</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Comment</td>
</tr>
<tr>
<td>ICJ Statute</td>
<td>Statute of the International Court of Justice</td>
</tr>
<tr>
<td>Abbreviations</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SCADA Systems</td>
<td>Supervisory Control and Data Acquisition Systems</td>
</tr>
<tr>
<td>Outer Space Treaty</td>
<td>Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and other Celestial Bodies</td>
</tr>
<tr>
<td>UNGA</td>
<td>United Nations General Assembly</td>
</tr>
<tr>
<td>UNSC</td>
<td>United Nations Security Council</td>
</tr>
<tr>
<td>Tehran Hostages Case</td>
<td>United States Diplomatic and Consular Staff in Tehran (United States of America v Iran)</td>
</tr>
<tr>
<td>UDHR</td>
<td>Universal Declaration of Human Rights</td>
</tr>
<tr>
<td>WSIS</td>
<td>World Summit on the Information Society</td>
</tr>
</tbody>
</table>