

## CYBER WARFARE



# CYBER WARFARE

## Military Cross-Border Computer Network Operations under International Law

Johann-Christoph WOLTAG



intersentia

Cambridge – Antwerp – Portland

Intersentia Publishing Ltd.  
Sheraton House | Castle Park  
Cambridge | CB3 0AX | United Kingdom  
Tel.: +44 1223 370 170 | Email: mail@intersentia.co.uk

*Distribution for the UK:*  
NBN International  
Airport Business Centre, 10 Thornbury Road  
Plymouth, PL6 7 PP  
United Kingdom  
Tel.: +44 1752 202 301 | Fax: +44 1752 202 331  
Email: orders@nbninternational.com

*Distribution for the USA and Canada:*  
International Specialized Book Services  
920 NE 58th Ave. Suite 300  
Portland, OR 97213  
USA  
Tel.: +1 800 944 6190 (toll free)  
Email: info@isbs.com

*Distribution for Austria:*  
Neuer Wissenschaftlicher Verlag  
Argentinerstraße 42/6  
1040 Wien  
Austria  
Tel.: +43 1 535 61 03 24  
Email: office@nwv.at

*Distribution for other countries:*  
Intersentia Publishing nv  
Groenstraat 31  
2640 Mortsel  
Belgium  
Tel.: +32 3 680 15 50  
Email: mail@intersentia.be

Cyber Warfare. Military Cross-Border Computer Network Operations under  
International Law  
Johann-Christoph Woltg

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

ISBN 978-1-78068-226-6  
D/2014/7849/59  
NUR 828

British Library Cataloguing in Publication Data. A catalogue record for this book is  
available from the British Library.

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

<i>Acknowledgements</i> .....	vii
<i>Abbreviations</i> .....	xv

<b>Introduction</b> .....	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

<b>Chapter 1. A Survey of Computer Network Operations</b> .....	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
<b>Chapter 2. The Legal Regime of Cyberspace . . . . .</b>	<b>53</b>
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

<b>Chapter 3. Computer Network Operations Outside of Armed Conflict . . . . .</b>	<b>85</b>
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>



## ABBREVIATIONS

Banjul Charter	African Charter on Human and Peoples' Rights
ACHR	American Convention on Human Rights
<i>Genocide Convention Case</i>	<i>Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Judgment)</i>
UN Charter	Charter of the United Nations
CNA	Computer Network Attack
CNO	Computer Network Operation
Hague Regulations of 1907	Convention concerning the Laws and Customs of War on Land and its Annex: Regulations Respecting the Laws and Customs of War on Land
Hague Convention V	Convention respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land
CCDCOE	Cooperative Cyber Defence Centre of Excellence
COE	Council of Europe
ccTLD	Countrycode Top-Level Domain
CIP	Critical Infrastructures Protection
St. Petersburg Declaration	Declaration Renouncing the Use in Time of War of Explosive Projectiles under 400 Grammes Weight
DDoS	Distributed Denial of Service
DNS	Domain Name System
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ENISA	European Network and Information Security Agency
fn.	Footnote
Geneva Convention III	Geneva Convention relative to the Treatment of Prisoners of War

Manual on Air and Missile Warfare	Humanitarian Policy and Conflict Research Manual on International Law Applicable to Air and Missile Warfare
ILC Articles on State Responsibility	ILC Articles on Responsibility of States for Internationally Wrongful Acts
ICT	Information and Communication Technologies
ICCPR	International Covenant on Civil and Political Rights
ICRC	International Committee of the Red Cross
ICTY	International Criminal Tribunal for the Former Yugoslavia
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ICANN	Internet Corporation for Assigned Names and Numbers
IP	Internet Protocol
<i>Israeli Wall Advisory Opinion</i>	<i>Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion)</i>
MPEPIL	Max Planck Encyclopedia of Public International Law
Joint Project Agreement	Memorandum of Understanding between the US Department of Commerce and ICANN
<i>Nicaragua Case</i>	<i>Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits)</i>
NATO	North Atlantic Treaty Organization
Additional Protocol I	Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts
Additional Protocol II	Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts
RIAA	Reports of International Arbitral Awards
RFC	Request for Comment
ICJ Statute	Statute of the International Court of Justice



SCADA Systems	Supervisory Control and Data Acquisition Systems
Tallinn Manual	Tallinn Manual on the International Law Applicable to Cyber Warfare
Outer Space Treaty	Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and other Celestial Bodies
UN Convention on the Law of the Sea	United Nations Convention on the Law of the Sea
UNGA	United Nations General Assembly
UNSC	United Nations Security Council
<i>Tehran Hostages Case</i>	<i>United States Diplomatic and Consular Staff in Tehran (United States of America v Iran)</i>
UDHR	Universal Declaration of Human Rights
WSIS	World Summit on the Information Society

