

FRANÇOIS DELERUE

CAMBRIDGE  
STUDIES IN  
INTERNATIONAL  
AND  
COMPARATIVE  
LAW

# Cyber Operations and International Law

CAMBRIDGE



p64  
488.50

สำนักหอสมุดมหาวิทยาลัยเชียงใหม่

164.6943  
124.92.51  
1 223874d3

# CYBER OPERATIONS AND INTERNATIONAL LAW

FRANÇOIS DELERUE

*Institut de Recherche stratégique de l'École militaire*



CAMBRIDGE  
UNIVERSITY PRESS

# CONTENTS

*List of Abbreviations*      xix

<b>1</b>	<b>Does International Law Matter in Cyberspace?</b>	<b>1</b>
1.1	Cyber International Law: New Challenges for International Law?	4
1.1.1	International Law Is Applicable to Cyberspace and Cyber Operations	6
1.1.1.1	International Air Law	7
1.1.1.2	International Space Law	8
1.1.1.3	International Cyberspace Law	9
	A Cyberspace Is Not a New Legal Domain	10
	B Nothing Prevents International Law from Applying to Cyber Activities	13
1.1.2	General Challenges to International Law: International Legality and Stability at Stake	13
1.1.2.1	The Failure of the Last UNGGE	14
1.1.2.2	From Discussions between Like-Minded States to Fragmentation of International Law	19
1.1.2.3	The Increasing Role of Non-state Actors in International Law-Making and Norm-Building Processes	21
1.1.2.4	Soft Law rather Than Hard Law	24
1.1.2.5	The Chimeric Debate on the Adoption of a New Treaty	26
1.1.2.6	Concluding Remarks on the General Challenges to International Law	27

1.2 The Scope of the Book	28
1.2.1 The Scope <i>Ratione Materiae</i> : Cyberspace and Cyber Operations	29
1.2.1.1 Cyberspace	29
1.2.1.2 Computer Networks and the Internet	29
1.2.1.3 The Nature of Cyber Operations	35
1.2.1.4 Cyber Operations as Part of a Composite Operation	36
1.2.2 The Scope <i>Ratione Personae</i> : State-Sponsored Cyber Operations	37
1.2.3 The Scope <i>Ratione Legis</i> : The Applicable Law	38
1.2.3.1 Critical Perspective on the Notion of Cyber Warfare	39
1.2.3.2 Contextualising State-Sponsored Cyber Operations under International Law	41
A Cyber Operations Occurring in Peacetime	41
B Cyber Operations Occurring during a Pre-existing Armed Conflict	42
C Cyber Operations Occurring during an Armed Conflict and Transforming Its Nature	43
1.3 The Contribution of the Book	44
1.4 The Content of the Book	48

## PART I Attribution

2 Attribution to a Machine or a Human: A Technical Process	55
2.1 Attribution to a Machine	56
2.1.1 How to Identify a Machine	57
2.1.1.1 Serial Number	57
2.1.1.2 MAC Address	58
A Definition	58
B Using MAC Addresses for Identification	60
C MAC Addresses Spoofing	61

2.1.1.3	IP Addresses	61
A	A Brief Introduction to IP Addresses	62
B	Using IP Addresses for Identification	65
C	IP Address Spoofing	67
(i)	IP Address Spoofing and DoS Attack	67
D	Conclusion Regarding IP Addresses	69
2.1.2	Techniques for the Attribution of Cyber Operations	69
2.1.3	Difficulties in the Process of Attribution	70
2.1.3.1	Multi-stage Cyber Operations	71
2.1.3.2	Conclusion Regarding Attribution to a Machine	71
2.2	Attribution to a Human	72
2.2.1	BadRabbit	73
2.2.2	The 2015 Cyber Operations against the Energy Sector in Ukraine	76
2.2.3	Cyber Operations against the Democratic National Committee (DNC)	78
2.2.4	People's Liberation Army (PLA) Unit 61398	80
2.2.5	Babar and Snowglobe	81
2.2.6	Stuxnet	82
2.2.7	DDoS attacks against Estonia	84
2.2.8	Conclusion Regarding Attribution to a Human	85
2.3	Concluding Remarks on Attribution to a Machine or a Human	85
3	<b>The Question of Evidence: From Technical to Legal Attribution</b>	87
3.1	State Practice on Evidence Relating to Cyber Operations	88
3.2	Evidence in International Law	91
3.3	Documentary Evidence	94
3.3.1	Typology of Documentary Evidence That May Be Collected in Relation to Cyber Operations	95



3.3.2	The Necessary Caution in the Collection and Assessment of Evidence	98
3.3.3	The Validity of Unlawfully Collected Evidence	100
3.4	Expert Opinion Evidence	103
3.4.1	Experts Appointed by the Parties	103
3.4.2	'Invisible' Experts Consulted by the Court	104
3.4.3	Experts Appointed by the Court	106
3.4.4	Assessors Appointed by the Court	107
3.5	Concluding Remarks on the Question of Evidence	108
4	Attribution to a State	111
4.1	Attribution of Cyber Operations Conducted by State Organs and Entities Empowered to Exercise Governmental Authority	114
4.1.1	Organs of State	115
4.1.1.1	<i>De Facto</i> Organs of a State	118
4.1.2	Entities Empowered to Exercise Elements of Governmental Authority	123
4.1.3	Organs Placed at the Disposal of Another State	125
4.1.4	<i>Ultra Vires</i> Cyber Operations	126
4.1.5	Conclusion Regarding Cyber Operations Conducted by State Organs and Entities Empowered to Exercise Governmental Authority	128
4.2	Attribution of Cyber Operations Conducted by Private Individuals	128
4.2.1	Cyber Operations Conducted under the Instructions, Direction or Control of the State	129
4.2.1.1	Distinction between <i>De Facto</i> Organ of the State and Acts Perpetrated under the Instructions, Direction or Control of the State	129
4.2.1.2	Diversity of Approaches on the Attribution of Acts Conducted under the Instructions, Direction or Control of the State	130
A	The ICJ's <i>Nicaragua</i> Case and the 'Effective Control' Test	130
B	The ICTY's <i>Tadić</i> Case and the 'Overall Control' Test	134

C	The Articles on State Responsibility	139
D	The <i>Armed Activities</i> and <i>Bosnian Genocide</i> Cases: Restating the 'Effective Control' Test	140
	(i) The <i>Armed Activities</i> Case	140
	(ii) The <i>Bosnian Genocide</i> Case	141
E	Analysing and Navigating the Various Approaches	143
4.2.1.3	Applying the Various Approaches to Cyber Operations	144
	A 2007 Estonia DDoS Attacks	146
	B Private Cybersecurity Companies	149
4.2.1.4	Conclusion Regarding Cyber Operations Conducted under the Instructions, Direction or Control of the State	150
4.2.2	Cyber Operations Conducted in the Absence or Default of the State	150
4.2.3	Cyber Operations Endorsed by the State	151
4.2.3.1	Stuxnet	154
4.2.3.2	Estonia	155
4.2.4	Cyber Operations Conducted in the Context of Mob Violence, Insurrections and Civil Wars	156
4.3	Autonomous Cyber Operations	157
4.3.1	The Place of Autonomous Cyber Operations in Policy	159
4.3.2	Hypothetical Examples of Autonomous Cyber Systems	161
4.3.3	Attribution of Autonomous Cyber Operations to the Launching State	162
4.3.4	Legal Questions Surrounding the Use of Autonomous Cyber Operations	162
4.3.5	Concluding Remarks on Autonomous Cyber Operations	164
4.4	State Practice on the Attribution of Cyber Operations to States	165
4.4.1	From Unilateral to Semi-collective and Collective Attribution	165
4.4.1.1	WannaCry	166
4.4.1.2	NotPetya	173

4.4.1.3	4 October 2018: The First Collective Attribution of Cyber Operations	178
4.4.1.4	From Collective Attribution to Collective Response	181
4.4.2	The Judicialisation of Attribution	182
4.4.3	Conclusion Regarding State Practice on Attribution	184
4.5	Concluding Remarks on the Attribution of Cyber Operations to a State	184
<b>Part I – Conclusion</b>		<b>189</b>

## **PART II The Lawfulness of Cyber Operations**

<b>5</b>	<b>Internationally Wrongful Cyber Acts: Cyber Operations Breaching Norms of International Law</b>	<b>193</b>
5.1	Cyber Operations as Inimical or Unfriendly Acts	193
5.2	The Absence of a Specific Legal Regime for Cyber Espionage	198
5.3	Cyber Operations and Territorial Sovereignty	200
5.3.1	Defining Territorial Sovereignty	201
5.3.1.1	State Sovereignty	201
5.3.1.2	Territorial Sovereignty	203
5.3.1.3	Territorial Sovereignty over Cyberspace and Computer Networks	206
5.3.1.4	States' Jurisdiction over Cyberspace	208
5.3.2	Cyber Operations Violating the Territorial Sovereignty of a State	209
5.3.2.1	Only a State Can Violate the Territorial Sovereignty of Another	210
5.3.2.2	Cyber Operations Penetrating a Foreign System	211
A	State Exercising Its Power on the Territory of Another State	214
B	The Absence of a Damage Requirement	215
C	Evolution and Contestation in the Approaches of Some States	219
D	The Nature of the Target and Means of Infection	222



E	Concluding Remarks on Cyber Operations Penetrating the Targeted System	225
5.3.2.3	Cyber Operations Not Penetrating a Foreign System	226
5.3.2.4	Involuntary Violation of Territorial Sovereignty	228
5.3.2.5	Cyber Operations Violating the Sovereignty of Numerous States: the Examples of WannaCry, NotPetya and BadRabbit	230
5.3.3	Conclusions Regarding Territorial Sovereignty	232
5.4	Cyber Operations and the Principle of Non-intervention and Non-interference	232
5.4.1	The Principle of Non-intervention and Non-interference	233
5.4.1.1	The Content of the Principle	234
5.4.1.2	The Various Forms of Intervention	237
5.4.1.3	The Practice before the ICJ	237
5.4.2	Cyber Intervention	238
5.4.2.1	The Principle of Non-intervention and Existing Examples of Cyber Operations	239
A	Sony Pictures Entertainment	239
B	Stuxnet	240
C	Estonia	241
5.4.2.2	Cyber Operations as Part of a Composite Influence Operation	241
A	The Distinction between Preparatory Actions and Composite Acts	242
B	The Hack of the Democratic National Committee during the 2016 US Presidential Election	244
C	The Hack of 'En Marche!' during the 2017 French Presidential Elections	250
D	Concluding Remarks on Cyber Operations and Influence Operations Aiming at Interfering in an Electoral Process	254
5.4.2.3	Cyber Intervention during a Civil War	257

5.4.2.4	Cyber Espionage and the Principle of Non-intervention	258
5.4.3	Concluding Remarks on the Principle of Non-intervention	259
5.5	Cyber Operations and Human Rights	260
5.5.1	The Applicability of Human Rights Law to Cyber Operations	261
5.5.2	Privacy in the Digital Age	264
5.5.3	Other Human Rights	268
5.5.4	Concluding Remarks on Cyber Operations and Human Rights	270
5.6	Concluding Remarks on the Lawfulness of State-Sponsored Cyber Operations	271
 6	 <b>The Threshold of Cyber Warfare: from Use of Cyber Force to Cyber Armed Attack</b>	 273
6.1	Cyber Operations and the Prohibition of the Use of Force	278
6.1.1	The Prohibition of the Use of Force	278
6.1.1.1	The Prohibition of the Use of Force and the International Court of Justice	279
6.1.1.2	The Prohibition of the Use of Force and the Principle of Non-intervention	280
6.1.1.3	The Status of the Prohibition of the use of Force under Customary International Law and <i>jus Cogens</i>	281
6.1.2	Cyber Operations as Prohibited Uses of Force	283
6.1.3	The Prohibited Force Is Not Confined to 'Armed Force'	284
6.1.4	Diversity of Approaches on 'Cyber Force'	288
6.1.4.1	The Target-Based Approach	288
6.1.4.2	The Instrument-Based Approach	289
6.1.4.3	The Consequence-Based Approach	289
6.1.5	The Criterion of 'Gravity' or 'Severity' of the Coercive Cyber Activity	290
6.1.5.1	The Threshold of Gravity of the Prohibited Use of Force	291
6.1.5.2	Cyber Operations and the Threshold of Gravity	294

6.1.5.3	The Distinction between Cyber Operations Producing Effects in the Real World and Those Producing Only Cyber Effects	296
6.1.6	Cyber Operations Targeting Critical Infrastructures	298
6.1.6.1	The Notion of Critical Infrastructures	299
6.1.6.2	Critical Information Infrastructures	302
6.1.6.3	Cyber Force and Critical Infrastructures	303
6.1.7	The Attribution of a Coercive Cyber Activity to a State and Its Intent	304
6.1.7.1	Attribution of the Coercive Cyber Activity Conducted by Proxies	305
6.1.7.2	Coercive Cyber Activities Executed by Mistake or Involuntarily	306
6.1.8	Relevant Circumstantial Evidence for the Qualification of a Coercive Cyber Activity as a Prohibited Use of Force	307
6.1.8.1	The Circumstances of the Coercive Cyber Activity	307
6.1.8.2	The Publicity of the Coercive Cyber Activity	308
6.1.9	Conclusion on Cyber Operations and the Prohibition of the Use of Force	310
6.2	Cyber Threat and Threat of Cyber Force	311
6.2.1	The Prohibition of the Threat of Force	312
6.2.2	Cyber Threat of Force	314
6.2.3	The Prohibition of the Threat to Resort to Prohibited Force	315
6.2.3.1	The ICJ's Formula	315
6.2.3.2	Open Threat to Resort to Cyber Force	317
6.2.4	Demonstration of Cyber Force as a Prohibited Threat of Force	319
6.2.4.1	Large-Scale Distributed Denial of Service Attacks as a Demonstration of Force	320
6.2.4.2	A Computer Worm Causing Non-physical Damage as a Demonstration of Force	322
6.2.4.3	A Computer Worm Causing Physical Damage as a Demonstration of Force	323
6.2.4.4	Military Exercises	324

6.2.5	Building Cyber Capabilities Does Not Constitute a Prohibited Threat of Force	325
6.2.6	Conclusion Regarding the Threat of Cyber Force	327
6.3	Cyber Armed Attack and Cyber Aggression	327
6.3.1	The Effects of Cyber Operations	331
6.3.1.1	The Consequences to Be Taken into Account	331
6.3.1.2	Cyber Operations Having Physical Consequences	332
6.3.1.3	Cyber Operations Having Only Non-physical Consequences	333
6.3.2	Accumulation of Cyber Operations Short of an Armed Attack	334
6.3.3	The Author of the Armed Attack	335
6.3.4	The Target of the Armed Attack	339
6.3.4.1	Cyber Operations Targeting Critical Infrastructures	341
6.3.5	Conclusion Regarding Cyber Armed Attack	342
6.4	Concluding Remarks on <i>Jus Contra Bellum</i> and Cyber Operations	342
7	<b>Circumstances Precluding or Attenuating the Wrongfulness of Unlawful Cyber Operations</b>	343
7.1	Cyber Operations Conducted with the Consent of the Affected State	345
7.2	<i>Force Majeure</i>	346
7.3	Distress	347
7.4	Necessity	348
7.5	Concluding Remarks on Circumstances Precluding Wrongfulness	351
8	<b>Cyber Operations and the Principle of Due Diligence</b>	353
8.1	Does a Duty to Prevent Any Use of State Cyber Infrastructures Exist?	358
8.1.1	A State Has No Obligation to Have Absolute Knowledge of All Events and Activities on Its Territory or in Cyber Infrastructures under Its Control	359

8.1.2	The Slippery Slope of Justifying Mass Surveillance	360
8.1.3	The Difference between Cyber Operations Launched from or Solely Transiting through the Territory of the State	362
8.2	The Absence of a Threshold of Harm	363
8.3	The Duty of a State to Take Measures to Terminate an Unlawful Cyber Operation Using Its Infrastructure	366
8.3.1	Knowledge of the Territorial State	366
8.3.2	Measures to Terminate the Cyber Operation	367
8.3.3	Distinction between State of Transit and State of Launch	368
8.4	Toward a Duty to Prevent the Potential Significant Transboundary Harm Caused by Cyber Operations	369
8.5	Toward a Duty to Disclose Zero-Day Vulnerabilities	371
8.6	Concluding Remarks on Cyber Due Diligence	374
	<b>Part II – Conclusion</b>	<b>377</b>

### **PART III Remedies against State-Sponsored Cyber Operations**

<b>9</b>	<b>State Responsibility and the Consequences of an Internationally Wrongful Cyber Operation</b>	<b>381</b>
9.1	Obligation of Cessation	382
9.1.1	The Obligation of Cessation in the Event of a Distributed Denial of Service Attack	385
9.1.2	The Obligation of Cessation Regarding the Intrusion of a Malware	386
9.1.3	Concluding Remarks on the Obligation of Cessation	388
9.2	Assurances and Guarantees of Non-repetition	388
9.3	Obligation of Making Reparation	392
9.3.1	Cyber Operations and the Notion of Injury	393
9.3.2	Causality	394
9.3.3	The Duty to Mitigate	395
9.3.4	The Different Forms of Reparation	399
9.3.4.1	Restitution	402

9.3.4.2	Compensation	405
A	Material Damage	407
(i)	Physical Damage Caused by Cyber Operations	407
(ii)	Non-physical Damage Caused by Cyber Operations	409
(iii)	Compensation for the Cost Resulting from the Removal of a Malware	410
B	Moral Damage	410
9.3.4.3	Satisfaction	412
9.3.4.4	Concluding Remarks on the Forms of Reparation	414
9.3.5	The Difficult Reparation of the Consequences of NotPetya	414
9.4	Shared Responsibility	416
9.4.1	An Injury Caused by a Plurality of Internationally Wrongful Acts of Several States	417
9.4.2	An Injury Caused by a Joint Internationally Wrongful Act of Several States	418
9.4.3	Concluding Remarks on Shared Responsibility	420
9.5	Concluding Remarks on State Responsibility and the Consequences of an Internationally Wrongful Cyber Operation	421
<b>10</b>	<b>Measures of Self-Help against State-Sponsored Cyber Operations</b>	<b>423</b>
10.1	Retorsion	424
10.1.1	Cyber Retorsion	426
10.1.1.1	Estonia and Georgia	427
10.1.1.2	Operation Ababil	428
10.1.1.3	State Practice on Measures of Retorsion	431
10.1.2	Concluding Remarks on Retorsion	432
10.2	Countermeasures	433
10.2.1	The Main Characteristics of Countermeasures	437
10.2.1.1	Unilateral Measures	437
10.2.1.2	Prior Wrongful Act	438



10.2.1.3	Inter-State Dimension	439
10.2.1.4	Reversibility	440
10.2.1.5	Objective of Countermeasures	441
10.2.1.6	Non-forcible Character of Countermeasures	442
10.2.2	Procedural Conditions	443
10.2.2.1	Call for Reparation and Notification	444
10.2.2.2	Urgent Countermeasures	445
10.2.3	Substantive Conditions	448
10.2.3.1	Necessity	448
10.2.3.2	Proportionality	448
10.2.3.3	Prohibited Countermeasures	451
10.2.3.4	Temporal Elements of Countermeasures	452
10.2.4	Third States and Countermeasures	453
10.2.4.1	Third States Affected by Countermeasures	453
10.2.4.2	Third States Conducting Countermeasures	454
	A Solidarity Measures	454
	B Measures in Response to a Violation of an <i>Erga Omnes</i> Obligation	457
10.2.5	Concluding Remarks on Countermeasures	460
10.3	Self-Defence	460
10.3.1	<i>Ratione Personae</i> Requirement	463
10.3.2	<i>Ratione Temporis</i> Requirement	465
10.3.2.1	Beginning of Self-Defence	466
	A Interceptive Self-Defence	468
	B Pre-emptive Self-Defence	472
	C Preventive Self-Defence	476
	D Concluding Remarks on the Beginning of Self-Defence and on Anticipatory Forms of Self-Defence	476
10.3.2.2	End of Self-Defence	477
10.3.3	<i>Ratione Conditionis</i> Requirement: Necessity and Proportionality	478
10.3.3.1	Necessity	479
10.3.3.2	Proportionality	481

10.3.3.3	Concluding Remarks on <i>Ratione Conditionis</i> Requirement	482
10.3.4	Remedies against Cyber Use of Force Short of an Armed Attack	483
10.3.4.1	Armed Reprisals against Use of Force Short of an Armed Attack	483
10.3.4.2	Accumulation of Cyber Operations Short of an Armed Attack	487
10.3.5	Concluding Remarks on Self-Defence	487
10.4	Concluding Remarks on Measures of Self-Help against State-Sponsored Cyber Operations	488
	<b>Part III – Conclusion</b>	<b>491</b>
11	<b>Conclusion</b>	<b>493</b>
	<b>Appendix – Table Assessing the Lawfulness of Cyber Operations and Potential Responses</b>	<b>499</b>
	<i>Select Bibliography</i>	502
	<i>Index</i>	509