CYBER OPERATIONS AND INTERNATIONAL LAW

This book offers a comprehensive analysis of the international law applicable to cyber operations, including a systematic examination of attribution, lawfulness and remedies. It demonstrates the importance of countermeasures as a form of remedies and also shows the limits of international law, highlighting its limits in resolving issues related to cyber operations. There are several situations in which international law leaves the victim State of cyber operations helpless. Two main streams of limits are identified. First, in the case of cyber operations conducted by non-state actors on the behalf of a State, new technologies offer various ways to coordinate cyber operations without a high level of organization. Second, the law of State responsibility offers a range of solutions to respond to cyber operations and seek reparation, but it does not provide an answer in every case and it cannot solve the problem related to technical capabilities of the victim.

FRANÇOIS DELERUE is a research fellow in cyber defence and international law at the Institute for Strategic Research (IRSEM – Institut de Recherche stratégique de l'École militaire) and an adjunct lecturer at Sciences Po Paris. He is also rapporteur on international law for the Academic Advisory Board of the project EU Cyber Direct.

CAMBRIDGE STUDIES IN INTERNATIONAL AND COMPARATIVE LAW: 146

Established in 1946, this series produces high quality, reflective and innovative scholarship in the field of public international law. It publishes works on international law that are of a theoretical, historical, cross-disciplinary or doctrinal nature. The series also welcomes books providing insights from private international law, comparative law and transnational studies which inform international legal thought and practice more generally.

The series seeks to publish views from diverse legal traditions and perspectives, and of any geographical origin. In this respect it invites studies offering regional perspectives on core *problématiques* of international law, and in the same vein, it appreciates contrasts and debates between diverging approaches. Accordingly, books offering new or less orthodox perspectives are very much welcome. Works of a generalist character are greatly valued and the series is also open to studies on specific areas, institutions or problems. Translations of the most outstanding works published in other languages are also considered.

After seventy years, Cambridge Studies in International and Comparative Law sets the standard for international legal scholarship and will continue to define the discipline as it evolves in the years to come.

Series Editors

Larissa van den Herik

Professor of Public International Law, Grotius Centre for International Legal Studies, Leiden University

Jean d'Aspremon

Professor of International Law, University of Manchester and Sciences Po Law School

A list of books in the series can be found at the end of this volume.

CYBER OPERATIONS AND INTERNATIONAL LAW

FRANÇOIS DELERUE
Institut de Recherche stratégique de l'École militaire

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314-321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi - 110025, India

79 Anson Road, #06-04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781108748353
DOI: 10.1017/9781108780605

First published 2020
First paperback edition 2021

A catalogue record for this publication is available from the British Library

ISBN 978-1-108-49027-6 Hardback
ISBN 978-1-108-74835-3 Paperback

CONTENTS

List of Abbreviations xix

1 Does International Law Matter in Cyberspace? 1

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 *Ratione Materiae*: 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 *Ratione Personae*: State-Sponsored Cyber Operations 37
1.2.3 The Scope *Ratione Legis*: 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 The Question of Evidence: From Technical to Legal Attribution 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 *De Facto* 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 *Ultra Vires* 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 *De Facto* 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 *Nicaragua* Case and the 'Effective Control' Test 130
B The ICTY's *Tadić* Case and the 'Overall Control' Test 134

C The Articles on State Responsibility 139
D The *Armed Activities* and *Bosnian Genocide* Cases: Restating the 'Effective Control' Test 140
(i) The *Armed Activities* Case 140
(ii) The *Bosnian Genocide* 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

Part I – Conclusion 189

PART II **The Lawfulness of Cyber Operations**

5 Internationally Wrongful Cyber Acts: Cyber Operations Breaching Norms of International Law 193

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 The Threshold of Cyber Warfare: from Use of Cyber Force to Cyber Armed Attack 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 *jus Cogens* 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 *Jus Contra Bellum* and Cyber Operations 342

7 Circumstances Precluding or Attenuating the Wrongfulness of Unlawful Cyber Operations 343

7.1 Cyber Operations Conducted with the Consent of the Affected State 345
7.2 *Force Majeure* 346
7.3 Distress 347
7.4 Necessity 348
7.5 Concluding Remarks on Circumstances Precluding Wrongfulness 351

8 Cyber Operations and the Principle of Due Diligence 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

Part II – Conclusion 377

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

9 State Responsibility and the Consequences of an Internationally Wrongful Cyber Operation 381

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

10 Measures of Self-Help against State-Sponsored Cyber Operations 423

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 *Erga Omnes* Obligation 457
10.2.5 Concluding Remarks on Countermeasures 460
10.3 Self-Defence 460
10.3.1 *Ratione Personae* Requirement 463
10.3.2 *Ratione Temporis* 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 *Ratione Conditionis* Requirement: Necessity and Proportionality 478
10.3.3.1 Necessity 479
10.3.3.2 Proportionality 481

10.3.3.3 Concluding Remarks on *Ratione Conditionis* 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

Part III – Conclusion 491

11 Conclusion 493

Appendix – Table Assessing the Lawfulness of Cyber Operations and Potential Responses 499

Select Bibliography 502
Index 509

ABBREVIATIONS

ADC	Anonymous Digital Coalition
AFDI	Annuaire français de droit international
AFRINIC	African Network Information Center
ANSSI	Agence nationale de la sécurité des systèmes d'information [National Cybersecurity Agency of France]
APNIC	Asia-Pacific Network Information Centre
APT	advanced persistent threat
ARIN	American Registry for Internet Numbers
ARP	Address Resolution Protocol
ARPANET	Advanced Research Project Agency Network
C&C	Command & Control
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CERN	European Organization for Nuclear Research
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency (USA)
CID	Company ID
CNA	computer network attack
CNE	computer network exploitation
CNO	computer network operation
CoE	Council of Europe
CSEC	Communications Security Establishment Canada
CSIRT	Computer Security Incident Response Team
DARPA	Defense Advanced Research Projects Agency (USA)
DDoS	distributed denial of service
DNC	Democratic National Committee (USA)
DoD	Department of Defense (USA)
DoS	denial of service
DrDoS	distributed reflection denial-of-service attack
ECI	European Critical Infrastructure
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDT	Electronic Disturbance Theater

EPCIP	European Programme for Critical Infrastructure Protection
EUI	European University Institute
EUI	Extended Unique Identifier
FRY	Federal Republic of Yugoslavia
FSB	Federal Security Service (Russian Federation)
FTP	File Transfer Protocol
GARR	Gruppo per l'Armonizzazione delle Reti della Ricerca [Italian academic and research network]
GCSB	Government Communications Security Bureau (New Zealand)
GCSC	Global Commission on the Stability of Cyberspace
GGE	Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of the United Nations
GOP	Grand Old Party (US Republican Party)
GRU	Main Intelligence Agency (Russian Federation)
IAC	international armed conflict
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICT	information and communications technology
IDF	Israel Defence Forces
IEEE	Institute of Electrical and Electronics Engineers
IHL	international humanitarian law
ILA	International Law Association
INRIA	Institut national de recherche en informatique et en automatique
IoT	Internet of Things
IP	Internet Protocol
IPv4	IP address version 4
IPv6	IP address version 6
Iran-US CTR	Iran-United States Claims Tribunal Reports
IRIA	Institut de recherche en informatique et en automatique
ISP	Internet Service Provider
ITC	International Tin Council
ITU	International Telecommunication Union
LACNIC	Latin America and Caribbean Network Information Centre
LAN	Local Area Network
LARS	Lethal Autonomous Robots
LAWS	Lethal Autonomous Weapons Systems
LGDJ	Librairie générale de droit et de jurisprudence
LIR	Local Internet Registry

MAC	Media Access Control
MLC	Mouvement de libération du Congo [Congo Liberation Movement]
MS	Member State(s)
NAT	network address translation
NATO	North Atlantic Treaty Organization
NCI	National Critical Infrastructure
NCIRC	NATO Computer Incident Response Capability
NCP	Network Control Protocol
NCSC	GCSB's National Cyber Security Centre (New Zealand)
NIAC	non-international armed conflict
NIC	Network Interface Controller
NIR	National Internet Registry
NK or N.K.	North Korea
NORSAR	Norwegian Seismic Array
NRO	Number Resource Organization
NSA	National Security Agency (USA)
OECD	Organisation for Economic Co-operation and Development
OIV	Opérateur d'importance vitale
OUI	Organizationally Unique Identifier
PLA	People's Liberation Army (PRC)
PMSC	private military and security company
PRC	People's Republic of China
RAND Corporation	Research AND Development Corporation (USA)
RBN	Russian Business Network
RCADI	Recueil des cours de l'Académie de droit international de La Haye [Collected Courses of the Hague Academy of International Law]
RIPE NCC	*Réseaux IP Européens* Network Coordination Centre
RIR	Regional Internet Registry
SAIV	Secteurs d'activités d'importance vitale
SCO	Shanghai Cooperation Organization
SFOR	Stabilization Force
SRI	Stanford Research Institute
Tallinn Manual	*Tallinn Manual on the International Law Applicable to Cyber Warfare*
Tallinn Manual 2.0	*Tallinn Manual on the International Law Applicable to Cyber Operations*
TAO	NSA's Office of Tailored Access Operations (USA)
TCP	Transmission Control Protocol
TRNC	Turkish Republic of Northern Cyprus
U/L bit	Universally/Locally administered address bit

UCLA	University of California in Los Angeles
UN Doc	Document of the Organization of the United Nations
UNEP	United Nations Environment Programme
UNGGE	Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of the United Nations
UNIDIR	United Nations Institute for Disarmament Research
UNUC	United Nations Operation in the Congo
URL	Uniform Resource Locators
USA or U.S.A	United States of America
USB	Universal Serial Bus
VRS	Army of Republika Srpska
WWW	World Wide Web
ZANL	Zapatista Army of National Liberation