

Leonhard Kreuzer

The Harm Prevention Rule in Cyberspace

An Obligation of Due Diligence



Nomos

Beiträge zum
ausländischen öffentlichen Recht und Völkerrecht

Edited by

the Max Planck Society
for the Advancement of Science
represented by Prof. Dr. Armin von Bogdandy
and Prof. Dr. Anne Peters

Volume 335

Leonhard Kreuzer

The Harm Prevention Rule in Cyberspace

An Obligation of Due Diligence



Nomos

Open Access funding provided by Max Planck Society.

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at <http://dnb.d-nb.de>

a.t.: Berlin, FU, Diss., 2022

ISBN 978-3-7560-1356-2 (Print)
978-3-7489-1884-4 (ePDF)

1st Edition 2024

© Leonhard Kreuzer

Published by

Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Production of the printed version:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN 978-3-7560-1356-2 (Print)
ISBN 978-3-7489-1884-4 (ePDF)
DOI <https://doi.org/10.5771/9783748918844>



Online Version
Nomos eLibrary



This work is licensed under a Creative Commons Attribution 4.0 International License.

Der Familie

Acknowledgements

This book is based on my doctoral thesis which the Faculty of Law of the Free University Berlin accepted in December 2022. For the publication, I updated case law, state practice and literature until May 2024.

I would like to thank my doctoral supervisor Prof. Dr. Heike Krieger for her continuous support, trust and encouragement. A special thanks is also due to my second doctoral supervisor Prof. Dr. Dr. h.c. Anne Peters for her helpful feedback and generous support. The joint work with both Prof. Dr. Krieger and Prof. Dr. Dr. h.c. Peters on our co-edited book ‘Due Diligence in the International Legal Order’ had a substantial impact on my writing process and I am very thankful for the experience.

I am furthermore grateful to the Max Planck Society for the Advancement of Science for financing my position as a Research Fellow at the Max Planck Institute for Comparative Public Law and International Law as part of the research group ‘Towards a Proceduralization of International Law?’, as well as for making the open access publication of this book possible. I would also like to thank the Free University Berlin for kindly hosting me as a researcher. The thesis has benefitted from constructive criticism in the research seminar of the Berlin Potsdam Research Group ‘The International Rule of Law – Rise or Decline?’ for which I am very thankful.

For including the book in the Max Planck Series „Contributions to Comparative and International Public Law“ I would like to extend my gratitude to Prof. Dr. Armin von Bogdandy and again to Prof. Dr. Dr. h.c. Anne Peters.

People who have accompanied me during the writing process have influenced the work on this book in their own ways. While I can name but a few I would like to thank Jonas Püschmann, Milan Tahraoui and Sofie-Marie Terrey for their friendship and helpful feedback on the thesis, Maximilian Schlang for many long conversations, my parents and my sister for their great support, and Elmira for being within everything.

Leonhard Kreuzer

Berlin, in June 2024

Table of Contents

List of Abbreviations	19
Introduction	21
Chapter 1: Current State of the International Legal Discourse on Cyber Harm	27
A. Popular categories of malicious cyber operations	27
I. Cyber espionage	27
II. Cyber terrorism	29
III. Cyber war	31
IV. Cyber attack	32
V. Cybercrime	33
VI. Imprecision of categorical terms	34
B. The concept of cyber harm	35
I. Cyber harm as exploitation of code vulnerability	35
II. Means of causing cyber harm	35
III. Exclusion: Human error, social engineering and content harm	37
C. Different degrees of cyber harm	39
I. Intrusive access operations: Loss of confidentiality	39
II. Disruptive operations: Impairment or loss of functionality	40
III. Destructive operations: Physical harm	40
IV. Other categorization of cyber harm effects	41
D. Current state of the international legal discourse	41
I. Gradual recognition of the applicability of international law in cyberspace	42
II. States' preference for strategic ambiguity	45
III. Filling the void: Non-state actor proposals	46
IV. Turn to preventive approaches against cyber security risks	47

Chapter 2: The Harm Prevention Rule in International Law	49
A. The harm prevention rule in international law	49
I. The evolution of the harm prevention rule in international law	49
II. Holistic protection of interests of other states	52
III. Territory, jurisdiction or control: Risk proximity as basis of accountability	53
IV. Knowledge of risk of harm required	55
V. The duty to exercise due diligence to prevent and mitigate harm	56
1. Due diligence as an obligation of conduct	56
2. The preventive and remedial dimension of due diligence	58
VI. The negative prohibitive dimension of the harm prevention rule	59
B. The harm prevention rule as the most suitable term for expressing the due diligence rationale	62
C. The doctrinal status of the harm prevention rule	66
I. The harm prevention rule as a customary rule of a general character	66
II. The harm prevention rule as a general principle of international law	67
D. Threshold of recognition in new areas of international law	69
I. The inductive approach and its limits	70
II. Complementary deductive considerations	71
III. Threshold for deductive considerations	73
IV. Endorsement of deductive considerations in cyberspace	75
V. Relevant state practice and opinio iuris in cyberspace	76
E. Recognition of the harm prevention rule in cyberspace by individual states	77
I. Momentum towards recognition of the rule	77
II. Concern and pushback	81
1. Concern about over-securitization	81
2. Capacity concerns	82

F. Recognition of the rule on the UN level	83
I. Endorsement of the harm prevention rule in the UN GGE Reports	83
II. Problematic terminology of the UN GGE Reports	85
1. Hortatory language of the UN GGE Reports	88
2. Permissive assertions of freedom of action	90
G. Need for specification in cyberspace	91
Chapter 3: The Threshold for Triggering Due Diligence Obligations to Prevent	95
A. General Criteria	95
I. Risk of significant cyber harm	95
II. Integrating acts reaching the threshold of prohibitive rules into the risk of harm threshold	100
III. Interpretation of risk of significant harm in cyberspace	102
IV. Non-physical harm as relevant harm under the harm prevention rule	103
V. Cumulative harm as relevant harm under the harm prevention rule	106
VI. Context-dependent flexible assessment of significant cyber harm	107
B. Acts reaching the threshold of prohibitive rules	107
I. Prohibition on the use of force	108
1. Recognition of the prohibition on the use of force in cyberspace	108
2. Acts amounting to a use of force in cyberspace	110
3. Application of the threshold to specific cyber incidents	114
4. The exceptional implication of the threshold of prohibited force in cyberspace	116
II. Prohibition of intervention	116
1. Recognition of the prohibition of intervention in cyberspace	116
2. <i>Domaine réservé</i>	118
3. The challenge of asserting coercion in cyberspace	119
3.1 Interference with elections	121
3.2 Intervention in the fundamental operation of parliament	122

3.3 Cyber operations against critical infrastructure	124
3.4 Impacts on the stability of the financial system	125
3.5 Harm to the political and/or cultural system	127
3.6 Undermining the territorial state's exclusive right to enforce the law	127
4. Lack of clarity regarding the threshold of prohibited intervention	129
III. Sovereignty	129
1. The suggestion of a sovereignty rule in cyberspace	129
2. Sovereignty as a fundamental principle of international law	131
3. 'Violations of sovereignty' in international practice	132
4. Concepts of sovereignty in cyberspace	134
5. Legal content of a prohibitive sovereignty rule in cyberspace	136
5.1 The absolutist 'pure' sovereigntist approach	136
5.2 Degree of infringement on territorial integrity	139
5.3 Interference with or usurpation of inherently governmental functions	141
5.4 Exercise of state power	143
5.5 Lack of sufficiently clear content of a sovereignty rule in cyberspace	144
6. Assessing risks and benefits of a sovereignty rule in cyberspace	145
C. Significant cyber harm beyond acts reaching the threshold of prohibitive rules	147
I. Economic cyber harm as a category of significant cyber harm	147
1. The problem of economic cyber harm	148
2. Increasing concern about economic cyber harm	149
3. Criteria for assessing the significance of economic harm	150
3.1 Violation of intellectual property rights and trade secrets	150
3.2 Further criteria for assessing the gravity of economic harm	154
4. Economic harm as an emerging category of significant cyber harm	155

II. Cyber harm to critical infrastructure as a category of significant cyber harm	156
1. Increasing concern about cyber operations against critical infrastructure	157
2. Diverging definitions of critical infrastructure	158
III. Increasing concern about harm to the public core of the internet	161
IV. Cyber espionage as a category of significant cyber harm	164
1. The legality of espionage in international law	165
2. Increasing concern about harm caused by mass surveillance operations	166
3. Increasing concern about cyber espionage operations against governmental and international institutions	171
V. Emerging legal yardsticks for risks of significant cyber harm	174
 Chapter 4: Negative and Positive Obligations under the Harm Prevention Rule	 177
A. The negative prohibitive dimension of the harm prevention rule	177
I. Restrictive formulation regarding attacks on critical infrastructure in the UN GGE Reports	177
II. States' negative obligations regarding all categories of significant cyber harm	181
B. Required standard for due diligence under the harm prevention rule in cyberspace	182
I. Due diligence as a capacity-dependent binding obligation of conduct	184
II. Due diligence vs. 'soft' best practice standards	185
III. Systematic interpretation of due diligence requirements in cyberspace	187
IV. The relevance of the duty to protect under international human rights law	188
V. Categories of due diligence measures	193
C. Procedural due diligence measures	194
I. Duty to cooperate	194
1. Cooperation in international law	195
2. Cooperation and due diligence	196

3. Cooperation in cyberspace	198
4. Focus on specific cooperative duties preferable	200
II. Duty to take action against ongoing or imminent harmful operations	201
1. Duty to take action and due diligence	201
2. Duty to take action in cyberspace	202
3. Knowledge	204
4. Required measures	205
5. Widespread support of a due diligence obligation to take action in cyberspace	208
III. Duty to notify	208
1. Duty to notify in international law and with regard to due diligence	208
2. Duty to notify in cyberspace	210
3. Reluctance of states to commit to a duty to notify in cyberspace	211
4. Nascent emergence of a due diligence obligation to notify in cyberspace	213
IV. Duty to cooperate on the prosecution of cybercrime	214
1. Prohibition of extraterritorial law enforcement as a challenge for cybercrime prosecution	215
2. Cooperation in legal instruments on cybercrime: Discussions on the UN level	216
3. Cooperation requirements in cybercrime treaties	217
4. Tracing international legal standards for cybercrime cooperation	219
4.1 Formal cooperation: Mutual legal assistance	219
4.2 Principles and limits of mutual legal assistance	220
4.3 Informal cooperation	222
5. The challenge of assessing cybercrime cooperation standards beyond a minimum standard	222
V. Risk mitigation measures regarding ICT vulnerabilities	223
1. Definition of ICT vulnerabilities	224
2. Exploitation of ICT vulnerabilities by intelligence and law enforcement	225
3. Vulnerability disclosure as a due diligence requirement	226
3.1 Reporting of ICT vulnerabilities	227
3.2 Information on remedies	230

4. Links of state exploitation to attacks on the integrity of the supply chain	231
5. The protection of the integrity of the supply chain in the UN GGE Report 2015	232
6. Emergence of best practice standards regarding ICT vulnerability disclosure	233
VI. Summary on procedural due diligence obligations	234
D. Due Diligence Measures Regarding a State's Institutional Capacity	235
I. Cybercrime legislation and prosecution	235
1. Criminal legislation and prosecution as due diligence requirements	236
2. Criminal legislation and prosecution under international human rights law	237
3. Assessing international standard on cybercrime legislation and prosecution	239
3.1 Criminalization requirements under cybercrime treaties	240
3.2 Convergence on an international minimum standard	246
4. Criminal procedural law as a due diligence requirement	246
4.1 Standard procedural measures	247
4.2 Divergences regarding human rights safeguards	248
4.3 Diverging capacities	250
4.4 The gradual emergence of an international minimum standard and associated risks	251
II. Level of actual or constructive knowledge under the harm prevention rule	252
1. No rebuttable presumption of knowledge	252
2. Duty to have known under the harm prevention rule	253
3. Content of a duty to have known in cyberspace	255
4. Practical implications	257
III. Critical infrastructure protection	259
1. Duty to protect own critical infrastructure against cyber harm	259
1.1 Spill-over effects of cyber harm to critical infrastructure	259
1.2 Duty to protect critical infrastructure under human rights law	261

1.3 Best practice standards for protecting critical infrastructure	262
1.3.1 Ensuring IT security standards	263
1.3.2 Criminal legislation	264
1.3.3 Inter-state and public-private cooperation	264
1.4 Non-binding best practice standards	265
2. Duty to prevent cyber harm to the critical infrastructure of other states	266
IV. The establishment of computer emergency response teams and points of contact for international cooperation	267
1. Divergent understandings of emergency response teams and points of contact	267
2. Establishment of CERTs and points of contact as a due diligence requirement	268
3. Establishment of CERTs and points of contact under binding and non-binding norms	270
V. Evolving due diligence standard regarding institutional capacity	272
Chapter 5: Enforcement of the Harm Prevention Rule	275
A. Legal consequences of negligence	275
I. Harm not a constituent element of an internationally wrongful act	277
II. Complementary applicability of the prevention rules and the rules on state responsibility	280
B. The content of state responsibility following negligence	282
I. Compensation and reparation in cases of cyber harm	282
II. Cessation	286
C. Countermeasures against negligence	287
I. Purpose and proportionality requirements	288
II. Notification requirement	290
III. Countermeasures against states	291
IV. The problem of collective countermeasures	292
V. The limited role of countermeasures for the enforcement of the harm prevention rule	294

Chapter 6: General Conclusions	297
A. The potential of the harm prevention rule in cyberspace	297
B. Central findings	301
Bibliography	307
Table of Cases	325

List of Abbreviations

ARSIWA	Draft Articles on the Responsibility of States for Internationally Wrongful Acts
ASEAN	Association of Southeast Asian Nations
AU	African Union
CBM	Confidence-building measure
NATO CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CoE	Council of Europe
CIA	Confidentiality, integrity and availability
COVID	Coronavirus SARS-CoV-2
DDoS	Distributed Denial of Service
ECtHR	European Court of Human Rights
EU	European Union
GCSC	Global Commission on the Stability of Cyberspace
IACtHR	Inter-American Court of Human Rights
ICJ	International Court of Justice
ICT	Information and communications technology
ILC	International Law Commission
ITU	International Telecommunications Union
MoU	Memorandum of Understanding
NAM	Non-Aligned Movement
NIS Directive	EU Directive on the security of network and information system, EU/2016/1148
NIS 2 Directive	EU Directive on measures for a high common level of cybersecurity across the Union, EU/2022/2555
NSA	National Security Agency
OAS	Organization of American States
OPCW	Organization for the Prohibition of Chemical Weapons
OSCE	Organization for Security and Co-Operation in Europe

List of Abbreviations

PCIJ	Permanent Court of International Justice
SCO	Shanghai Cooperation Organization
UN Charter	Charter of the United Nations
UN GGE	UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
UN ODC	UN Office of Drugs and Crime
UN OEWG	UN Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security
TRIPS	WTO Agreement on Trade-Related Aspects of Intellectual Property Rights
WTO	World Trade Organization