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

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

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

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

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

Introduction

Hardly a week goes by without reports about major malicious cyber incidents.[1] Cyber incidents adversely affect nation states, but often have an even regional or global scale. The widespread use of malicious cyber tools by both state and non-state actors creates serious risks that endanger international peace and security and harm societies, organisations, businesses and individuals.

International law has so far struggled to deliver an effective normative framework to counter cyber insecurity and is frequently perceived as underdeveloped.[2] A multilateral cyber security treaty is not in sight.[3] Only a few legally binding treaties on cybercrime exist.[4] Frequently, legal commitments of states are non-binding, informal, or ambiguous. Particularly technologically powerful states have adopted a 'wait and see' strategy[5] of 'ambiguity and silence'.[6]

Furthermore, for a significant amount of time the international legal discourse was dominated by the cyberwar narrative[7] – i.e. the notion that an

1 For a continuously updated overview of significant cyber incidents (focusing on cyber operations against government agencies, defence and high tech companies and economic crimes with losses of more than a million dollars) see Center for Strategic and International Studies, 'Significant cyber incidents', available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents; 119 significant cyber incidents were reported for 2023 alone.

2 Kubo Mačák, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers ', *Leiden Journal of International Law* 30 (2017), 877–899.

3 On dim prospects in this regard Rebecca Crootof, 'International Cybertorts: Expanding State Accountability in Cyberspace', *Cornell Law Review* 103 (2018), 565–644, at 640–642.

4 See on cybercrime treaties and cybercrime legislation more generally chapter 4.D.

5 Harriet Moynihan, 'The Application of International Law to State Cyberattacks Sovereignty and Non-intervention', *Chatham House – Research Paper*, 2019, para. 23.

6 Dan Efrony/Yuval Shany, 'A Rule Book on the Shelf ? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice', *The American Journal of International Law* 112 (2018), 583–657, at 588.

7 See e.g. Andrei Khalip, 'U.N. chief urges global rules for cyber warfare', *Reuters,* 19 February 2018, citing UN Secretary General Guterres: 'I am absolutely convinced that, differently from the great battles of the past, which opened with a barrage of artillery or aerial bombardment, the next war will begin with a massive cyber attack to destroy military capacity (…) and paralyse basic infrastructure such as the electric networks', available at: https://www.reuters.com/article/us-un-guterres-cyber-idUSKCN1G31Q4.

armed confrontation conducted solely or predominantly via cyber means is imminent. As a consequence, the legal discourse has so far primarily focused on applicable legal rules for reactions to violations of international law. Yet, such a reactive approach faces two notorious problems:

First, the threshold for a violation of the prohibition on the use of force, as well as for a prohibited intervention is met only in exceptional cases. Cyber operations frequently lack the comparability in 'scale and effects' to a traditional military operation[8], hereby falling short of a prohibited use of force. Cyber operations also frequently lack the element of coercion required for a violation of the prohibition on intervention as they often occur clandestinely or wreak havoc without bending the will of a state.[9] If and which international legal norms apply to so-called 'low-level' cyber operations – i.e. operations below the violation threshold of the two above-mentioned norms – is hence so far not sufficiently clear.

Second, even if a cyber operation reaches the threshold of a violation of one of the two norms international law regularly only provides a recourse for states if the act is attributable to a state. Yet, reliable and timely attribution – a legal requirement for taking countermeasures against a state – is notoriously problematic in cyberspace.[10]

Both problems have led to the concern of a cyber 'wild west'[11], a 'lawless lacuna'[12] and more generally a crisis of international law in cyber-

8 The scale and effects threshold asserted by the ICJ, *Military Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment of 27 June 1986, ICJ Reports 1986, p. 14, 103, para. 195, has also been acknowledged by states in cyberspace, see e.g. the then legal adviser to the US Department of State Harold Hongju Koh, 'International Law in Cyberspace', *Harvard International Law Journal* 54 (2012), 4.

9 In more detail on the threshold of a prohibited intervention in the cyber context see chapter 3.B.II.

10 On flaws and gaps in the existing methodology Nicholas Tsagourias/Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges', *European Journal of International Law* 31 (2020), 941–967, at 967; on the notoriety of the attribution problem Henning Christian Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge: Cambridge University Press 2020), 109, 110.

11 Michael N. Schmitt/Liis Vihul, 'Respect for Sovereignty in Cyberspace', *Texas Law Review* 95 (2017), 1639–1670, at 1670; François Delerue, 'Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace', in Taťána Jančárková/Lauri Lindström et al. (eds.), *Going Viral* (NATO CCDCOE 2021), 9–24, at 24.

12 Luke Chircop, 'A Due Diligence Standard of Attribution in Cyberspace', *International and Comparative Law Quarterly* 67 (2018), 1–26, at 11.

space.[13] A prohibitive norm against low-level cyber harm (i.e. cyber harm below the threshold of a prohibited intervention) is hence perceived as central for enhancing cyber stability.[14]

A prominent proposal in this regard was a suggestion by the Tallinn Manual[15] that sovereignty as such constitutes a prohibitive primary rule in cyberspace.[16] If a cyber operation does not reach the threshold of a prohibited use of force or intervention, this sovereignty rule with a lower violation threshold could apply residually and hereby rein in malicious state-sponsored cyber operations that would otherwise go unheeded by international law. However, from the outset, also a sovereignty rule in cyberspace can counter malicious cyber operations only to a limited extent for two reasons: First, it again requires the notoriously problematic attribution of malicious acts to a state.[17] Second, it only entails a negative obligation on states to refrain from acts that would violate the sovereignty of other states. It does not address the risk emanating from non-state actors in cyberspace and in particular does not require a state to rein in malicious operations of non-state actors. The potential of a sovereignty rule for curbing international cyber harm comprehensively is hence limited from the outset.[18]

Thus, another rule of international law has increasingly come into the focus of states and commentators: The rule that is often referred to as the principle or obligation of 'due diligence' or the duty not to cause and to prevent significant harm – which this study refers to as the harm prevention

13 Highlighting indicators of a crisis of international law but cautioning against such an assessment Mačák, 'From Cyber Norms to Cyber Rules' 2017 (n. 2), 5f.

14 Przemysław Roguski, '*Violations of Territorial Sovereignty in Cyberspace – an Intrusion-Based Approach,*' in: Dennis Broeders/Bibi van den Berg (eds.), *Governing Cyberspace: Behaviour, Power and Diplomacy* (London: Rowman & Littlefield 2020), 65–84, at 80.

15 A group of international legal experts convened under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). The group produced two Manuals: Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge: Cambridge University Press 2013) and Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press 2017).

16 Michael N. Schmitt (ed.), 'Tallinn Manual 2.0' 2017 (n. 15), Rule 4: 'A State must not conduct cyber operations that violate the sovereignty of another State'. It is important to note that the Tallinn Manual is an expert manual and lacks legal authority as the Manual itself acknowledges, see ibid., Introduction, p. 2.

17 Tsagourias 'Cyber Attribution' (n. 10Lahmann, 'Unilateral Remedies' 2020 (n. 10), 16.

18 In more detail on a potential sovereignty rule in cyberspace see chapter 3.B.III.

rule.[19] This rule has been asserted in the *Island of Palmas, Corfu Channel* and *Trail Smelter* cases[20] and requires states to exercise due diligence to prevent harm emanating from their territory or under their control to the legally protected interests of other states.[21] If a state acts negligent, e.g. by failing to intervene with the acts of malicious non-state actors operating on its territory, it is held accountable, not for the actual malicious act itself, but for its negligence in preventing or mitigating it.

Two advantages seem to make this rule a potent legal tool against low-level cyber harm: First, it bypasses the notorious attribution problem. For finding a violation of the due diligence requirement it is not necessary that the malicious act is attributable to the state. Proof of mere negligence suffices.[22] Second, the primary focus of due diligence is prevention and mitigation of risks of harm, instead of reaction and retaliation. This is attractive in cyberspace as reactions to cyber attacks, aside from the attribution problems mentioned above, face strict legal limits, such as time, purpose or proportionality, that make reactions to cyber operations frequently inefficient or impractical.[23]

The promise of the due diligence rationale under the harm prevention rule is hence to provide an accountability mechanism against low-level cyber harm and to incentivize risk resilience and emergency preparedness. States and commentators have increasingly highlighted its potential to make cyberspace more stable and secure.[24] A comprehensive analysis of the application and implementation of the norm in cyberspace is however lacking so far.[25] The present study aims to undertake such a comprehensive analysis.

---

19 On terminology in more detail see chapter 2.B; on due diligence in international law see Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020).

20 See *Island of Palmas Case (Netherlands v. United States of America)*, Award of 4 April 1928, PCA Case No. 1925–01, p. 9, Vol. II, p. 829 at p. 839; *Trail Smelter Case (United States v. Canada)*, Decisions of 16 April 1938 and 11 March 1941, vol. III, UNRIAA, 1905–1982, at 1965; ICJ, *Corfu Channel Case (United Kingdom v. Albania)*, Judgment of 9 April 1949, ICJ Reports 1949, 4, p. 22.

21 In more detail see chapter 2.

22 In more detail see chapter 5.A.I.

23 Lahmann, 'Unilateral Remedies' 2020 (n. 10), 200: '[Countermeasures] will rarely be available as a remedy aimed at protection for the targeted state (…)'; in more detail on the strict legal limits for reactions to cyber incidents under international law see chapter 5.C.I.

24 See in more detail chapter 2.E, F.

25 The report of Talita Dias/Antonio Coco, *Cyber Due Diligence in International Law* (Print version: Oxford Institute for Ethics, Law and Armed Conflict 2021) also sub-

To this aim, chapter 1 provides an overview of the current state of the international legal discourse regarding cyber threats. It contextualizes categorical terms such as cybercrime, cyber espionage or cyber attack, carves out their common characteristics, their differences, and differentiates between different harmful effects of cyber operations. It furthermore introduces the notion of cyber harm which is central for this study's focus on (cyber) harm prevention. The chapter highlights inherent structural challenges for the application of international law in cyberspace which have troubled reactive approaches to cyber harm but also play a role with regard to the harm prevention rule.

Chapter 2 introduces the harm prevention rule in international law and its due diligence aspects, highlighting its historical evolution, as well as its complex doctrinal and terminological character. It analyses to what extent states have recognized the rule's applicability in cyberspace. In doing so, it carves out the necessary threshold of state practice and opinio iuris. Chapter 3 then elaborates under which circumstances due diligence obligations to prevent and mitigate cyber harm are triggered. It highlights that states do not only need to act in the case of a risk of cyber harm that reaches the threshold of a specific prohibitive rule but also in other cases of significant cyber harm. Zooming into specific requirements, chapter 4 delineates which measures states are required to take to discharge their due diligence obligations. This analysis covers both procedural due diligence obligations, as well as due diligence obligations to take institutional safeguard measures against risks of cyber harm.[26] The study differentiates between due diligence obligations which can already be considered the required minimum standard and emerging standards of diligent conduct that may develop to binding due diligence standards in the future. Chapter 5 analyses the legal consequences of a violation of due diligence under the harm prevention rule and highlights the challenges of enforcing compliance with the rule. In conclusion, chapter 6 assesses the potential and limits of

stantively engages with the rule. Its rich analysis however deviates in scope. It only in some part analyses the harm prevention rule but extends its analysis to the analysis of due diligence obligations in international human rights law, as well as in international humanitarian law. It does not comprehensively cover the threshold triggering due diligence obligations, due diligence requirements in concreto, or the enforcement aspect of the harm prevention rule.

26 In more detail on these two main categories of due diligence obligations in international law see Anne Peters/Heike Krieger/Leonhard Kreuzer, 'Due diligence: the risky risk management tool in international law', *Cambridge Journal of International Law 9* (2020), 121–136, 124; see also below chapter 4.B.V.

the harm prevention rule for reducing cyber threats and making cyberspace more resilient and secure. It thereby touches upon the question whether international law can live up to its aspiration to foster international peace and security in cyberspace.

Chapter 1: Current State of the International Legal Discourse on Cyber Harm

To assess the current state of the international legal discourse regarding cyber threats it is important to understand the nature of cyber threats. Hence, the following section first outlines popular categorical terms for cyber operations before the concept of cyber harm which this study uses is introduced. The study then gives an overview of the current state of the international legal discourse on cyber harm.

A. Popular categories of malicious cyber operations

Both in the international legal discourse, as well as in media reports, a variety of incidents are reported as 'cyber' incidents, making 'cyber' something of a modern buzzword for any operation that involves the use of a computer system or the internet. In particular, categorical terms based on the intention or the affiliation of the attacker are popular. As outlined in the following, such categories are frequently imprecise and hence need to be approached with caution from the legal perspective.

I. Cyber espionage

Various cyber operations have the purpose to access and exfiltrate confidential information via cyber means. Operations for this purpose are traditionally labelled cyber espionage.[1] Cyber espionage operations are typically

1 Russell Buchan, 'The International Legal Regulation of Cyber Espionage', in Anna Maria Osula/Henry Rõigas (eds.) *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCD COE Publications 2016), 65–86, at 65: 'Espionage is a prevalent method of gathering intelligence and describes 'the consciously deceitful collection of information, ordered by a government or organisation hostile to or suspicious of those the information concerns, accomplished by humans unauthorised by the target to do the colleting.'; Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press 2017), commentary to rule 32, p. 168, para. 2: 'Cyber espionage involves, but is not limited

distinguished into two main categories. Espionage operations conducted by states for intelligence gathering – so-called 'political espionage' – and espionage operations by private actors for commercial reasons – so-called 'economic cyber espionage'. Noteworthy examples of political espionage include the *SolarWinds* operation, infiltrating inter alia the US Ministry for Nuclear Safety and the Defence Ministry in 2020[2], or the hack of the German parliament (Bundestag) in 2015 which compromised the servers of a significant number of parliamentarians.[3] Other espionage operations cannot always be neatly allocated to one of the two categories. For example, the allegedly state-sponsored vaccine espionage operations targeting vaccine research during the Coronavirus SARS-CoV-2 (COVID)-pandemic[4] was arguably conducted for both political as well as economic purposes.

Cyber espionage operations typically affect the confidentiality of information on information and communications technology (ICT) systems and networks but usually do not affect the integrity of data or cause disruption. It is often in an attacker's interest that the intrusion remains undetected so that exfiltration of information can continue as long as possible. On the technical level, cyber espionage is hence arguably the least intrusive mode of malicious cyber operations.[5] Nevertheless, it is important to note that it can have severe harmful effects: The exfiltration of classified information via cyber espionage can for example affect national security. Theft of intellectual property can cause great financial damage. Cyber espionage operations can also greatly interfere with the privacy of individuals.[6] Furthermore, once an attacker gains access to an ICT system

---

to, the use of cyber capabilities to surveil, monitor, capture, or exfiltrate electronically transmitted or stored communications, data, or other information.'.

2 David E. Sanger/Nicole Perlroth/Eric Schmitt, '*Scope* of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit', *New York Times,* 9 September 2021, available at: https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.

3 'Data stolen during hack attack on German parliament, Berlin says', *DW News*, 29 May 2015, available at: https://www.dw.com/en/data-stolen-during-hack-attack-on-german-parliament-berlin-says/a-18486900.

4 Dan Sabbagh/Andrew Roth, 'Russian state-sponsored hackers target Covid-19 vaccine researchers', *Guardian* 16 July 2020, available at: https://www.theguardian.com/world/2020/jul/16/russian-state-sponsored-hackers-target-covid-19-vaccine-researchers.

5 Luke Chircop, 'Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0', *Melbourne Journal of International Law* 20 (2019), 349–377, 359, 360.

6 Anne Peters, 'Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part II', *EJIL:Talk!*, 4 November 2013, available at: https://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-i/; UN General

during a cyber espionage operation it may only be the first step before the attacker wreaks further havoc, e.g. by altering or deleting data.[7] States are hence increasingly concerned about cyber espionage in international relations.[8]

II. Cyber terrorism

In the public and international legal discourse the term cyber terrorism is repeatedly used. Although a uniform definition does not exist cyber terrorist attacks are characterized by the intent of the attacker to spread fear and intimidation among the civilian population, through the cyber-induced occurrence of significant harm to physical objects or injury or death to individuals.[9] Both the UN Group of Governmental Experts (UN GGE) Reports 2021 as well as a 2017 UN Security Council Resolution acknowledged the threat of cyber terrorist attacks against critical infrastructure.[10] The risk

---

Assembly Resolution A/RES/68/167, 18 December 2013: 'Deeply concerned at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights (…)'.

7 Przemysław Roguski, *'Violations of Territorial Sovereignty in Cyberspace – an Intrusion-Based Approach',* in: Dennis Broeders/Bibi van den Berg (eds.), *Governing Cyberspace: Behaviour, Power and Diplomacy* (London: Rowman & Littlefield 2020), 65–84, at 75, 76; see also below chapter 1.C.I.

8 See in more detail chapter 3.C.IV.

9 Along these lines Irina Rizmal, 'Cyberterrorism: What are we (not) talking about?', *Diplo,* 3 August 2017, available at: https://www.diplomacy.edu/blog/cyberterrorism-what-are-we-not-talking-about :'For an attack to constitute an act of terrorism, it must also have a serious intended effect in terms of human and economic casualties or intense fear and anxiety – terror – among citizens'.

10 United Nations, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UN GGE), A/76/135, 14 July 2021 (UN GGE Report 2021), para. 13: 'The Group reaffirms that the use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security'; reiterating United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), A/70/174, 22 July 2015 (UN GGE Report 2015), para. 6; with regard to protection of critical infrastructure UN Security Council Res. 2341, 13 February 2017: 'Recognizing that protection efforts entail multiple streams of efforts, such as (…) cybersecurity'. See also generally

of cyber terrorist activities was also highlighted in a UN Office for Drugs and Crime (UN ODC) report.[11]

Yet, the label cyber terrorism is frequently overused. Terrorist groups have so far not shown great interest in malicious cyber operations.[12] No cyber terrorist attack has yet occurred that would fit the characteristic features of cyber terrorism – which is the causation of severe cyber-induced damage to spread fear and intimidation among the civilian population.[13] While e.g. the targeting of several Israeli websites, e.g. of the national airline and the disclosure of credit card details of Israeli citizens in 2012 were likened to cyber terrorism[14] the operation fell short of causing widespread fear, or severe casualties. Furthermore, activities like disseminating terrorist content, recruiting for and financing of terrorist organization, such as al-Qaida, via cyberspace are often misleadingly framed as cyber terrorism.[15] Even if such activities are eventually conducted for terrorist purposes they merely utilize cyberspace but do not attack it.[16] The label 'cyber' terrorism hence frequently does not fit. Due to this potential for misunderstanding this study uses the term cyber terrorism only cautiously.

on the subject International Law Association, *Study Group on Cybersecurity, Terrorism, and International Law,* 31 July 2016.

11 United Nations Office on Drugs and Crime (UN ODC), *The use of the Internet for terrorist purposes* (United Nations 2012).

12 David P. Fidler, 'Cyberspace, Terrorism and International Law', *Journal of Conflict & Security Law* 21 (2016), 475–493, at 478.

13 Rizmal, 'Cyberterrorism' 2017 (n. 9).

14 UN ODC, 'The Use of the Internet' 2012 (n. 11), 12.

15 See already James Lewis, 'Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats', Center for Strategic and International Studies, 2002, p. 4; also critical on this expansive use of the term Rizmal, 'Cyberterrorism' 2017 (n. 9): '[T]he label 'cyberterrorist' in the political discourse has mainly been applied to actors and organisations already framed as terrorist, despite recognising that these actors have not yet carried out activities that could be labelled as cyberterrorism'.

16 On the distinction between operations attacking the confidentiality, integrity and availability of ICT and operations merely utilizing ICT for other malicious purposes see below chapter I.B.III.

III. Cyber war

The threat of a looming cyberwar has dominated the international legal discourse for a significant amount of time.[17] Bolstering the cyberwar narrative both the NATO and the US have defined cyberspace as the fifth domain of warfare[18] – regardless of the fact that cyberspace is a fictitious notion as you cannot 'go into' cyberspace.[19] While operations in cyberspace have become an important operational field during armed conflict – as the war in Ukraine after the Russian invasion in February 2022 shows[20] – so far, a cyber war in the sense of an armed confrontation primarily conducted by cyber means has not yet occurred and it seems unlikely that this will change in the future.[21]

In order to amount to a forceful confrontation a cyber operation would need to amount to a prohibited use of force prohibited under Art. 2 (4) of the Charter of the United Nations (UN Charter) which would be the case if it is comparable in 'scale and effects' comparable to kinetic attacks.[22] Some operations have likely reached this threshold, such as the *Stuxnet* operation

17 See above Introduction; see the extensive amount of literature on cyberwar, e.g. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge: Cambridge University Press 2013), Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations Under International Law* (Intersentia 2014); Julia Dornbusch, *Das Kampfführungsrecht im internationalen Cyberkrieg* (Baden-Baden: Nomos 2018); Sven-Hendrik Schulze, *Cyber-»War« – Testfall der Staatenverantwortlichkeit* (Tübingen: Mohr Siebeck 2015); Li Zhang, 'A Chinese Perspective on Cyber War', *International Review of the Red Cross* 94 (2012), 801–807.

18 On the character of cyberspace as a domain of warfare and the function of this 'foundational metaphor' serving particular interests within the US military, e.g. with regard to the establishment of the US Cyber Command, Jordan Branch, 'What's in a Name? Metaphors and Cybersecurity', *International Organization* 75 (2021), 39–70, at 48.

19 Also critical of the characterization of cyberspace as a domain of warfare François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press 2020), 11.

20 During the Russian invasion of Ukraine cyber operations were primarily used to demoralize and spread disinformation, see Friedel Taube, 'Russia-Ukraine conflict: What role do cyberattacks play?', *Deutsche Welle*, 28 February 2022, available at: https://www.dw.com/en/russia-ukraine-conflict-what-role-do-cyberattacks-play/a-60945572.

21 Thomas Rid, *Cyber Will Not Take Place*, (London: Hurst 2017).

22 Harold Hongju Koh, 'International Law in Cyberspace', *Harvard International Law Journal* 54 (2012), 4.

against Iran in 2010 which disabled centrifuges in a nuclear enrichment facility in Natanz and arguably could have led to casualties, or the *Black Energy* operation against Ukraine which disabled part of a Ukrainian region's electricity grid.[23] Yet, such operations were singular cyber operations and did not lead to an ongoing armed confrontation primarily conducted via cyberspace.

Nevertheless, the term cyber war is invoked in an inflationary manner in situations which clearly fall short of an armed confrontation between states. The *SolarWinds* operation – an espionage operation lacking any destructive effect – has e.g. been likened to an act of cyber war.[24] Also the interference in the US presidential election in 2016 and potentially *any* form of state-sponsored cyber misconduct have been framed as an act of cyber war.[25] Such examples show that in the political discourse the term 'cyberwar' has become a placeholder for mere cyber confrontation or conflicts of states, conducted in cyberspace.[26] From a legal perspective the notion of cyber war hence needs to be approached with great caution as well.

IV. Cyber attack

Closely connected to the notion of cyber war is the notion of cyber attack. The Tallinn Manual defines the term as cyber operations that cause 'injury or death to persons or damage or destruction to objects'.[27] Such a definition of the term hence limits it to acts which likely amount to a use of force. Other definitions have a broader scope: *Brown* and *Tullos* for example

23 See in more detail on a violation of the prohibition of the use of force chapter 3.B.I.

24 Yevgeny Vindman, 'Is the SolarWinds Cyberattack an Act of War? It Is, If the United States Says It Is', *JustSecurity*, 26 January 2021, available at: https://www.lawfareblog.com/solarwinds-cyberattack-act-war-it-if-united-states-says-it.

25 Jordan Robertson/Laurence Arnold, 'Cyberwar: How Nations Attack Without Bullets or Bombs', *Washington Post*, 14 December 2020, available at: https://www.washingtonpost.com/business/energy/cyberwar-how-nations-attack-without-bullets-or-bombs/2020/12/14/878f2e88-3e43-11eb-b58b-1623f6267960_story.html.

26 Leonhard Kreuzer, 'Hobbesscher Naturzustand im Cyberspace? Enge Grenzen der Völkerrechtsdurchsetzung bei Cyberangriffen', in Ines-Jacqueline Werkner/Niklas Schörnig (eds.), *Cyberwar – die Digitalisierung der Kriegsführung* (Wiesbaden: Springer 2019), 63–86, at 69.

27 Schmitt, 'Tallinn Manual 2.0' 2017 (n.1), rule 92.

define cyber attacks as any cyber operation that causes physical damage[28], without indicating that a particular threshold of physical damage needs to be met. Even broader, France employs the term for any kind of hacking.[29] Other commentators have included the motivation of a malicious actor as a decisive element for a characterization as a cyber 'attack'.[30] Due to these largely divergent understandings using this term can likely lead to misunderstandings.[31] This study will hence also avoid it to the largest extent possible.

V. Cybercrime

Cybercrime operations are typically pursued by private actors for economic gain. The term is usually not used for state-sponsored cyber operations.[32] Examples of cybercrime operations are the ransomware attacks against the meat-processing company JBS in July 2021 by the cybercrime group REVil[33] or the theft of research data on COVID vaccines from an Oxford University research institute by a cybercrime group in February 2021.[34]

Cybercrime is a broad term that covers a variety of activities conducted against or via ICT for economic gain. The most popular means of cybercrime are operations which infiltrate or disrupt the orderly functioning of computer systems and networks via technical means – i.e. so-called 'hacking'.[35] But the cybercrime offences under cybercrime treaties also include

28 Gary D. Brown/Owen W. Tullos, 'On the Spectrum of Cyberspace Operations', *Small Wars Journal*, 11 December 2012, available at: https://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations.

29 France, Strategic Review of Cyber Defence, 2018, p. 4.

30 Oona Hathaway et al, 'The Law of Cyber Attack', *California Law Review* 100 (2012), 817–885, 836f.

31 Also arguing for caution with regard to the term Michael N. Schmitt, 'Terminological Precision and International Cyber Law', *Articles of War,* 29 July 2021, available at: https://lieber.westpoint.edu/terminological-precision-international-cyber-law/.

32 Henning Christian Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge: Cambridge University Press 2020), 20.

33 On the operation against JBS see the list of significant cyber incidents and the entries for May 2021 available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

34 The group subsequently sold the acquired data internationally, see ibid. in the entries for February 2021.

35 In more detail on 'hacking' and the concept of cyber harm see below chapter 1.B.

content-related offences, such as propaganda, or copyright-related offences, or computer-related offences, e.g. electronic fraud.[36] The term cybercrime hence carries a certain ambiguity. On the one hand, it is very broad and even includes offences which are merely conducted via cyberspace. On the other hand, it excludes state-sponsored cyber operations. As cybercrime is an established legal term, in particular employed by cybercrime treaties, this study will refer to cybercrime when suitable, albeit mindful of its definitional complexity.

VI. Imprecision of categorical terms

The above-mentioned examples show that popular terms for categorizing cyber operations have to be approached with caution. In particular, the terms cyber terrorism, cyber war and cyber attack are not based on a precise legal distinction but cover a wide variety of activities which deviate if and how they target ICT systems and networks. Only the term cyber espionage grasps activities that largely resemble one another on the technical level. For all categories the main distinguishing criterion is an attacker's motivation or affiliation.[37] As the preventive approach requires diligence measures against 'all hazards'[38], regardless of motivation or affiliation of an attacker, it is consequent that this study will largely avoid such motivation-based terminology. It will only refer to cyber espionage and cybercrime operations when suitable and more frequently refer to the neutral term 'cyber operations' or 'cyber incidents'[39], as well as to the umbrella notion 'cyber harm'. This notion is introduced in the following.

---

36 The Budapest Convention on Cybercrime distinguishes between four categories of cybercrime: offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences; copyright-related offences; see in more detail chapter 4.D.I; see also ITU, *Understanding cybercrime: Phenomena, challenges and legal Response* (ITU 2012), 12.

37 Lahmann, 'Unilateral Remedies' 2020 (n.32), 19.

38 Eneken Tikk/Kadri Kaska/Liis Vihul, International Cyber Incidents – Legal Considerations (NATO CCDCOE 2010), p. 10; Stein Schjolberg/Solange Ghernaouti-Hélie, *A Global Treaty on Cybersecurity and Cybercrime* (2nd edition, Oslo: AiTOslo 2011), p. 32.

39 Nevertheless, with regard to some categories of cyber harm the motivation of the attacker is at least a relevant factor to be taken into account, e.g. with regard to the intent to coerce under acts amounting to a prohibited intervention, see chapter 3.B.II.

B. The concept of cyber harm

I. Cyber harm as exploitation of code vulnerability

From cyber war, to cybercrime, to cyber terrorism to cyber espionage – on the core technical level all such cyber operations largely look alike: They exploit vulnerabilities in the design of ICT. ICT hardware, software and networks, including the internet, operate via code. Such code – often a line of millions of 1's and 0's[40] – inevitably entails errors which attackers can use to gain entry to a computer system or control a computer or data stored on it. Errors in code hence open the door to the compromising of the so-called 'CIA triad'. The CIA triad protects the confidentiality (C), integrity (I) and the availiability (A) of ICT systems and networks: Confidentiality protects against unauthorized access of the data stored in ICT systems and networks.[41] Integrity means that the stored data is complete and not improperly modified.[42] Availability means that authorized users should be able to access data upon request.[43] The compromising of one or several aspects of the CIA triad[44] is typically called 'hacking'. It is what this study understands as 'cyber harm'. Cyber harm is hence a broad umbrella term that largely grasps the activities traditionally framed under the above-mentioned categorical terms.[45]

II. Means of causing cyber harm

The exploitation of code vulnerabilities typically occurs through various stages. Attackers often first identify targets and vulnerabilities (so-called

40 Ryan Dube, 'What Is Binary Code and How Does It Work?', Lifewire, 2 March 2022, available at: https://www.lifewire.com/what-is-binary-and-how-does-it-work-4692749.

41 Chad Perrin, 'The CIA Triad', *TechRepublic,* 30 June 2008, available at: https://www.techrepublic.com/article/the-cia-triad/.

42 Josh Frühliner, 'The CIA triad: Definition, components and examples', *CSO Online*, 10 February 2020, available at: https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html.

43 Ibid.

44 If e.g. an attacker erases data all three aspects of the CIA triad are compromised: The erased data was accessed without authorization, was improperly modified and as a consequence is not accessible upon request anymore.

45 See above chapter 1.A.I–VI.

reconnaissance phase[46]), such as through probing or mapping[47], before they move towards exploiting found vulnerabilities by infiltrating a server and potentially taking control of it.[48] The most common tool which is used to compromise the CIA of ICT is malware. Malware is a catch-all term for different kinds of software designed to harm or exploit a computer, server or computer network, whether it is a virus, a worm, a Trojan horse, or ransomware.[49]

While a comprehensive list of various types of malware is not feasible, suffice it to highlight several particularly prominent types of malware that are repeatedly mentioned in the legal and political discourse and in the course of this study: 'Trojan horses' and more generally 'spyware' are often used to gain access to and copy data. They are hence regularly used for espionage purposes. 'Ransomware' is an increasingly popular tool for cybercriminals to extort money from victims. This type of malware encrypts data on the victim's hard drive; in order to regain access to the data the attacker demands payment of a ransom. Ransomware operations are hence akin to digital extortion. Another popular attack mode is a Distributed Denial of Service attack (DDoS) by which an attacker gains control over a huge number of infiltrated servers. Using this 'botnet' of infiltrated 'zombie' servers the attacker sends so many mass requests to a targeted server that the latter collapses.[50] While such operations primarily exploit vulnerabili-

46 Roguski, 'Territorial Sovereignty' 2020 (n. 7), 75.

47 Woltag, 'Cyber Warfare' 2014 (n. 17), 28.

48 On the seven stages of so-called cyber kill chains see Eric Hutchins/Michael J. Cloppert/Rohan M. Amin, 'Reconnnaisance, Weaponization, Delivery, Exploitation, Installation, Command and Control and Action on objective', in *Information Warfare & Security Research* 1 (2011), 1–14, at 5; see also Roguski, 'Territorial Sovereignty' 2020 (n. 7).

49 Microsoft, Robert Moir, *Defining Malware*, 2009; ITU Toolkit for Cybercrime Legislation, February 2010, section 1(n), p. 12, 13: 'malware may be defined as a program that is inserted into a computer program or system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the computer program, data or system.'; see the definition of malware by Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), glossary, 2.0, 566: 'Software' [that] may be stored and executed in other software, firmware, or hardware that is designed adversely to affect the performance of a computer system. Examples of malware include Trojan horses, 'rootkits', 'viruses' and 'worms'.'; Woltag, 'Cyber Warfare' 2014 (n. 17), 28.

50 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), glossary, 2.0, 565: '[DDoS is a] technique that employs multiple computing devices (e.g., computers or smartphones), such as the bots of a 'botnet' (…)), to cause a 'denial of service' [i.e. the non-availability of computer system resources to their users, addition by the author] to a single or multiple targets.'.

ties of the 'zombie' servers they simultaneously affect the availability of information on the targeted servers.[51]

Beyond these examples other forms of exploitation of vulnerabilities via malware are conceivable. For this reason the Convention on Cybercrime of the Council of Europe (CoE) – the so-called 'Budapest Convention' – deliberately entails broad offences which focus on the *effect* on the victim's ICT, instead of naming the use of specific forms of malware as offences.[52] Due to this effect-dependency the offences stipulated by various cybercrime treaties are adaptable to unknown, new types of malware.[53]

III. Exclusion: Human error, social engineering and content harm

The CIA triad is not only compromised through the exploitation of code via malware. Often, it is facilitated or enabled by human error. ICT users for example often use insecure passwords that can be guessed, or fall prey to so-called social engineering attacks. Social engineering can trick victims into entering passwords or other confidential information, e.g. by sending so-called phishing emails. With the acquired information attackers can subsequently gain access to a system or network in a subsequent step and hereby compromise the CIA triad. Many attackers consider social engineering attacks even more efficient than gaining access via purely technical means.[54] From the preventive perspective of this study the compromising of the CIA triad via social engineering is distinct as it involves active

51 Cybercrime Convention Committee (T-CY), T-CY Guidance Note, T-CY (2013)29, 8 October 2013, p.7.

52 The Council of Europe Convention on Cybercrime, 23 November 2001, ETS 2001, No. 185, stipulates the following broad offences: Illegal access (Art. 2), illegal interception (Art. 3), system interference (Art. 4), data interference (Art. 5); see in more detail chapter 4.D.I.

53 Cybercrime Convention Committee, T-CY (2013)29, 8 October 2013, p. 17: 'The numbers and variety of forms of malware are so vast that it would not be possible to describe even currently-known forms in a criminal statute. The Cybercrime Convention deliberately avoids terms such as worms, viruses, and trojans. Because fashions in malware change, using such terms in a Convention would quickly make it obsolete and be counterproductive.'

54 A cyber operation against a German steel mill was e.g. facilitated by social engineering, see on this e.g. Allianz Global Corporate & Specialty, *Cyber attacks against critical infrastructure*, available at: https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html.

recklessness on the side of the victim. It is hence excluded from this study's notion of cyber harm.

The study's notion of cyber harm also excludes offences which are committed via the means of a computer but do not target the CIA of ICT itself. Such malicious activities committed via the help of the internet are e.g. terrorist propaganda, hate speech or child pornography, or dissemination of 'fake' news'. The dissemination of disinformation during the COVID-pandemic, the interference in the US presidential elections in 2016 and 2020, or online hate speech against the Rohingya in Myanmar were e.g. frequently discussed as 'cyber' attacks or cyber harm.[55]

Yet, in these constellations ICT is only the means by which harm is amplified and disseminated but it is *not* the actual target itself. Using cyberspace to disseminate information leaves the CIA of ICT fully intact. The target is rather the human perception. Such content-based security risks are hence of a fundamentally different character than the ICT-vulnerability based notion of cyber harm.[56] While there is broad consensus on the illegitimacy and illegality of hacking it is far more contested which content is considered harmful in the international order. Deeming information harmful (or socially or politically destabilizing) has the risk to be abused by authoritarian governments to curb political dissent.[57] Information that is considered harmful in one state may be entirely uncontroversial and legitimate

55 Tom Burt, 'New Cyberattacks Targeting U.S. Elections', *MicrosoftBlog,* 10 September 2020, available at: https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/; Talita Dias/Antonio Coco*, Cyber Due Diligence in International Law* (Print version: Oxford Institute for Ethics, Law and Armed Conflict 2021), 90, 91.

56 See Leonhard Kreuzer, 'Disentangling the Cyber Security Debate', *Völkerrechtsblog*, 20 June 2018, available at: https://voelkerrechtsblog.org/de/disentangling-the-cyber-security-debate/.

57 On risks of counter-disinformation measures for freedom of expression Carme Colomina/Héctor Sanchez Margalef/Richard Youngs, 'The Impact of Disinformation on Democratic Processes and Human Rights in the World', *Study Requested by the DROI subcommittee* (European Parliament), April 2021, p. 16. For an overly broad definition of harmful information see e.g. China, National Cyberspace Security Strategy, 27 December 2016: 'Harmful information on the Internet erodes cultural security. Various ideological and cultural networks on the Internet are in conflict and confrontation, and excellent traditional culture and mainstream values are facing impact. Internet rumors, decadent culture and obscenity, violence, superstition and other harmful information that violates the core values of socialism (…) endanger cultural security'.

use of the freedom of expression in another state.[58] It is hence important to distinguish cyber harm from content-based information harm. While some international legal studies have implemented such a distinction[59], it is also frequently neglected in the international legal discourse.[60]

C. Different degrees of cyber harm

It is important to distinguish different degrees of cyber harm. Regardless of whether one frames a cyber operation under categorical terms such as cyber espionage, cyber war or cyber terrorism, the following three categories serve as analytical yardsticks in this regard.

I. Intrusive access operations: Loss of confidentiality

Intrusive access operations lead to the loss of confidentiality of data and the information this data embodies. They infiltrate an ICT system or network and typically copy data saved on it. Classical access operations are hence espionage operations. Usually access operations leave the integrity of data intact. One may hence be inclined to assess access operations as cyber harm of a lower intensity. Yet, while such an assumption may be apt in some cases, assuming a general presumption in this vein would go too far. On the one hand, access operations are often only a preparatory step before more disruptive steps are taken.[61] On the other hand, improperly acquired information can subsequently be published and hereby aggravate the harmful effect of a loss of confidentiality, e.g. through so-called doxing

58 Under international human rights law restrictions on free speech in cyberspace must comply with the requirements of legality, legitimacy, proportionality and necessity, UN Human Rights Committee, General Comment No. 34, CCPR/C/GC/34, 12 September 2011, para. 22.

59 The study group of the ILA has for example also implemented such a distinction, ILA, 'Cybersecurity and Terrorism' 2016 (n. 10), p. 2, para. 5.

60 A rare example from state practice in which a state argued for a distinction between cyber harm and content-based information risks is the statement by the Netherlands in the UN OEWG where it argued for an exclusion of disinformation problems which were 'outside of the scope of th[e] working group', Netherlands, The Kingdom of the Netherlands' response to the pre-draft report of the UN OEWG, 2020, p. 2, para. 15.

61 Roguski, 'Territorial Sovereignty' 2020 (n. 7), at 75, 76; this risk is typically associated with cyber espionage operations, see already above chapter 1.A.I.

operations in which malicious actors publish acquired personal data. Also access operations can hence already lead to severe harmful effects.

II. Disruptive operations: Impairment or loss of functionality

Disruptive cyber operations affect the functionality of a computer system or network. Examples are e.g. cyber operations which slow down the operation of a single server or a computer system; or DDoS attacks which cause the crashing of a server hosting a website[62], or ransomware attacks which encrypt files and hereby disrupt the orderly functioning of the computer system. Loss of functionality may hence be caused by a variety of malware types. Like the previous category of loss of confidentiality also the category of loss of functionality is limited to ICT-*internal* effects.

III. Destructive operations: Physical harm

Although the vast majority of cyber operations are access or disruptive operations some cyber operations can also have impacts 'in the real world beyond the cyber system itself'.[63] With regard to such ICT-*external* harm persons, physical objects or infrastructure are attacked '*through* cyberspace'.[64] An example of physical harm was e.g. the *Stuxnet* operation. In this case, malware manipulated the operation of centrifuges in an Iranian uranium enrichment facility and hereby led to their physical impairment.[65] Another example of physical cyber harm is the cyber-enabled impairment of medical equipment, e.g. during the COVID-pandemic, or the cyber-enabled crash of a car. Also physical damage to the ICT hardware itself may be considered physical cyber harm. It seems justified to consider physical harm as cyber harm when the resulting physical harm is sufficiently causally connected to the compromising of the CIA triad. Physical harm can also

62 Eleonora Viganò/Michele Loi/Emad Yaghmaei, 'Cybersecurity of Critical Infrastructure', in Markus Christen Bert Gordijn Michele Loi (eds.) *The Ethics of Cybersecurity* (Berlin: Springer Nature 2020), 157–178, 165.

63 Brown/Tullos, 'Cyberspace Operations' 2012 (n. 28).

64 Marco Roscini, 'Military Objectives in Cyber Warfare', in Mariarosaria Taddeo/Ludovica Glorioso (ed.), *Ethics and Policies for Cyber Operations* (NATO CCDCO 2017), 99–114, at 103.

65 On the operation see also Delerue, 'Cyber Operations' 2020 (n. 19), 2020, 407.

affect the functionality of cyber operations and hereby simultaneously have disruptive effects.[66] The increasing popularity of 'smart' objects connected to the internet and the use of artificial intelligence will likely heighten vulnerabilities for ICT-external harm in the future.[67]

IV. Other categorization of cyber harm effects

Other commentaators have developed more finely grained scale charts of different effects, distinguishing e.g. seven different degrees of effects[68], or between 'secondary' harm manifesting on the infrastructure controlled by ICT and 'tertiary' physical harm to individuals and objects as a consequence of the failure of the ICT infrastructure[69], or between harm to software, hardware, data and persons.[70] Again others merely distinguish between two categories of effects – 'functional' and 'physical' cyber harm[71], or 'physical and non-physical' effects.[72]

Yet, the three different categories of harmful effects outlined by this study on the one hand allow for a nuanced approach regarding ICT-internal harm by distinguishing between loss of confidentiality and loss of functionality. On the other hand, they also allow to compactly grasp various degrees of cyber harm, regardless of the specific malware used. This nuanced but compact categories of various degrees of cyber harm are best suited to assess the significance of cyber harm under the harm prevention rule.

D. Current state of the international legal discourse

To contextualize the current discussions on the harm prevention rule in cyberspace and cyber harm more generally it is important to be aware

66 Viganò/Loi/Yaghmaei have framed this as 'physical-functional' harm, 'Cybersecurity' 2020 (n. 62), 166.

67 On the risk of disabling cars via cyber means Bruce Schneier, 'Class Breaks', *Schneier on Security*, 3 January 2017, available at: https://www.schneier.com/blog/archives/2017/01/class_breaks.html; see also Viganò/Loi/Yaghmaei, 'Cybersecurity' (n. 62), 166.

68 Chircop, 'Territorial Sovereignty' 2019 (n. 5), 359, 360.

69 Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press 2014), 52.

70 Coco/Dias, 'Cyber Due Diligence Report' 2021 (n. 55), 72f.

71 Viganò/Loi/Yaghmaei, 'Cybersecurity' (n. 62), 166.

72 Delerue, 'Cyber Operations' 2020 (n. 19), 36.

of the inherent structural challenges for international law in cyberspace. These challenges are partially the reason for the underdeveloped status quo of international law in cyberspace and have partially caused the above-mentioned problems of reactive approaches.[73] Yet, they also play a role regarding the application and implementation of the harm prevention rule and hence need to be highlighted.

I. Gradual recognition of the applicability of international law in cyberspace

Already the technical design of cyberspace is a challenge for international law. Cyberspace is a decentralized network. A large number of private actors manage and operate most of the physical ICT infrastructure. The Internet Engineering Task Force e.g. develops core internet standards and protocols.[74] The seamless flow of data is enabled by settlement-free peering of private actors and packet-switched private networks.[75]

This seamless flow of data creates an ubiquity of cyberspace that is largely based on the technical community[76] and bypasses the state as a regulatory actor.[77] Due to its borderless technical character cyberspace has even been likened to a global commons.[78] Furthermore, non-state actors not only have a vital role in cyberspace as technical architects and operators but also as threat actors. Due to the interconnectedness of cyberspace even single attackers can wreak tremendous havoc. For example, a young attacker with limited hacking skills exposed the private addresses of a

73 See Introduction.

74 Internet Engineering Task Force, *DIG Watch,* available at: https://dig.watch/actors/internet-engineering-task-force.

75 Policy Brief: Internet Interconnection, *Internet Society*, 30 October 2015, available at: https://www.internetsociety.org/policybriefs/internetinterconnection/; Center for Democrary & Technology, 'ETNO Proposal Threatens Access to Open, Global Internet', 21 June 2012, available at: https://cdt.org/insights/etno-proposal-threatens-access-to-open-global-internet/, p. 3: 'The flow of communications between networks is (…) achieved through unregulated commercial agreements (…)'.

76 Dennis Broeders, *The Public Core of the Internet* (Amsterdam: Amsterdam University Press 2015), 11.

77 Milton L. Mueller, 'Against Sovereignty in Cyberspace', *International Studies Review* 22 (2020), 779–801, at 790.

78 Ibid., 794; Woltag has however convincingly pointed out that cyberspace should not be framed as a global commons as it is not an area outside of national jurisdiction, Woltag, 'Cyber Warfare' 2014 (n. 17), 56.

number of German parliamentarians following a cyber operation.[79] These aspects challenge the concept of 'supreme authority and territory'[80] under the concept of sovereignty, as well as of the state as a main threat vector on which international law is based.[81]

Hence, it was initially debated whether international law, or even domestic law, should apply in cyberspace.[82] Inter alia due to the work of the UN Group of Governmental Experts (UN GGE) – a group of selected governmental experts established by the UN General Assembly[83] – this debate is largely over. Cyberspace is based on physical components, e.g. on fibre-optic cables, routers, servers, as well as individuals acting in cyberspace. This 'physical layer'[84] of cyberspace is widely seen as the connecting link to the jurisdiction of the territorial state and consequently its regulation under international law. The UN GGE recognized in several consensual reports that the principle of territorial jurisdiction over the physical ICT infrastructure located on a state's territory, as well as international law more generally,

79 Grace Dobush, '20-year-old German Hacker Confesses in Doxxing Case', *Handelsblatt*, 1 August 2019, available at: https://www.handelsblatt.com/english/politics/data-leak-20-year-old-german-hacker-confesses-in-doxxing-case/23841212.html?ticket=ST-5094425-QxFvHBqs49OdjSVXp2nm-cas01.example.org. Acknowledging the cyber threat from non-state actors UN GGE Report 2021, para. 14: 'The Group also reaffirms that the diversity of malicious non-State actors, including criminal groups and terrorists, their differing motives, the speed at which malicious ICT actions can occur and the difficulty of attributing the source of an ICT incident all increase risk.'

80 Jens Bartelson, 'Dating Sovereignty', *International Studies Review* 20 (2018), 509–513, at 510.

81 On the challenge of such structural developments for the application of existing international legal rules see Heike Krieger/Georg Nolte, 'The International Rule of Law – Rise or Decline? Points of Departure', in Heike Krieger/Georg Nolte/Andreas Zimmermann (eds), *The International Rule of Law – Rise or Decline? – Approaching Current Foundational Challenges* (Oxford University Press 2019) 3–30, 15.

82 An infamous declaration assessed cyberspace outside the grasp of international law, John Perry Barlow, A Declaration of Independence for Cyberspace (1996), available at: http://w2.eff.org/Misc/Publications/ John_Perry_Barlow/barlow_0296.declaration.txt.

83 The group was first established in 2004 following UN General Assembly Resolution A/RES/58/32, 8 December 2003, para. 4.

84 Antal Berkes, 'Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control', *Israel Law Review* 52 (2019), 197–231, 201; Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 1, para. 4; Harriet Moynihan, 'The Application of International Law to State Cyberattacks Sovereignty and Non-intervention', *Chatham House – Research Paper*, 2019, para. 42.

applies.[85] No state hence seriously questions the general applicability of international law and the UN Charter in cyberspace anymore. While some states still argue for the development for new rules for cyberspace[86] the understanding prevails that such new rules would evolve as additional rules to the existing rules.[87]

Yet, a lack of certainty remains as to *how* existing rules of international law apply, including with regard to the harm prevention rule. Furthermore, the problem of non-state actors as important threat vectors lingers on with regard to the enforcement of international law. Due to the problem of attribution and technical evidence it is notoriously difficult to trace the source of a malicious cyber operation, at least in a timely manner.[88] Even if the server from which an attack presumably was conducted is identified the evidence may have been manipulated. While states have attributed cyber operations to states, as in the case of the attribution of the *WannaCry* attack to North Korea, such attribution constituted political attribution which did not meet the required standards of legal attribution.[89] The attribution

85 United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013 (UN GGE Report 2013), para. 20: 'State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.' This assertion was reiterated in the UN GGE Report 2015 and the UN GGE Report 2021, para. 71 lit. b.

86 China's Positions on International Rules-making in Cyberspace, October 2021: 'The international community should *develop* (emphasis added) universally accepted norms, rules and principles within the framework of the UN, to jointly address the risks and challenges, and uphold peace, security and prosperity in cyberspace.'

87 UN GGE Report 2021, para. 16: 'The Group also underscores the inter-relationship between norms, confidence-building measures, international cooperation and capacity-building. Given the unique attributes of ICTs, the Group reaffirms the observation of the 2015 report that additional norms could be developed over time, and, separately, notes the possibility of future elaboration of additional binding obligations, if appropriate.'; UN OEWG, Final Report 2021, para. 29: 'Given the unique attributes of ICTs, States reaffirmed that, taking into account the proposals on norms made at the UN OEWG, additional norms could continue to be developed over time. States also concluded that the further development of norms, and the implementation of existing norms were not mutually exclusive but could take place in parallel.'

88 See already above in the Introduction.

89 Kristen Eichensehr, 'Three Questions on the WannaCry Attribution to North Korea', *JustSecurity*, 20 December 2017, available at: https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/; states themselves distinguish between political and legal attribution see Netherlands, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the internation-

problem leads to an accountability gap that presents a persisting problem for the enforcement of international law in cyberspace.

II. States' preference for strategic ambiguity

A further structural problem for international legal progress was states' reluctance to commit to legally binding rules. While a significant number of states has in recent years published their opinio iuris on the applicability of international law in cyberspace[90] and has contributed to the inclusive UN Open-Ended Working Group (OEWG), established by the UN General Assembly in 2018, ambiguity remains. In statements on international law in cyberspace states frequently walk a fine line between asserting the applicability of international law, inter alia for deterrent purposes, but avoiding to commit to norms that may limit their ability to conduct offensive cyber operations themselves. A variety of states has asserted sovereignty as a prohibitive primary rule of international law but omitted to specify criteria for a violation of such a rule.[91]

States' strategic avoidance of accountability mechanisms also explains their preference for informal and non-binding norms. Instead of asserting binding legal rules, the UN GGE Reports for example assert '*non-binding*, *voluntary* norms of *responsible* state behaviour'.[92] As these norms largely reiterate existing binding rules of international law their categorization as non-binding creates an ambiguity that may undermine the legal force of international law in cyberspace on the mid-term.[93] While the recent inten-

al legal order in cyberspace, Appendix, International Law in Cyberspace, p. 6; for an overview of political attribution in state practice see Christina Rupp/Alexandra Paulus, *Official Public Political Attribution of Cyber Operations – State of Play and Policy Options* (Stiftung Neue Verantwortung 2023), 60.

90 See e.g. Finland, International law and cyberspace, Finland's national positions, October 2020; Iran, Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace, July 2020; New Zealand, The Application of International Law to State Activity in Cyberspace, 1 December 2020; France, International Law Applies to Operations in Cyberspace, September 2019; Germany, On the Application of International Law in Cyberspace, March 2021.

91 See in more detail chapter 3.B.III.

92 UN GGE Report 2015 stipulates norms, rules and principles (Part III, paras. 15–68), as opposed to international law (Part IV, paras. 69–73).

93 On the risk of diluting the binding character of existing legal obligations in cyberspace through the extensive use of hortatory language see below chapter 2.F.II.1.

sification of the international legal discourse is to be welcomed – the UN OEWG mandate was extended until 2025[94] and the UN GGE agreed on a consensual report[95] – it remains to be seen to what extent these processes can lead to norm acknowledgment, stabilization and internalization. With regard to the noteworthy but reluctant final results of both the UN GGE Report 2021[96] and the UN OEWG[97] it seems unlikely that states' appetite for specific and binding rules in cyberspace will grow significantly in the near future.

III. Filling the void: Non-state actor proposals

Due to the slow progress on the inter-state level non-state actors have advanced norm assessments and proposals and hereby partially filled the void of international law in cyberspace. Microsoft proposed a digital Geneva Convention and has put forward proposals on cyber norms.[98] The Global Commission on the Stability of Cyberspace (GCSC) proposed norms on advancing cyber stability.[99] Under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) a group of international law experts convened and produced two detailed manuals on the applicability of international law in cyberspace.[100] In December

94 UN General Assembly Resolution A/RES/75/240, 31 December 2020, paras. 1–4.

95 After the failure of the UN GGE Report 2017 the consensual report of 2021 is a significant step. See highlighting the positive aspects of the UN Report Michael N. Schmitt, 'The Sixth United Nations GGE and International Law in Cyberspace', *JustSecurity,* 10 June 2021, available at: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.

96 The UN GGE Report 2021 e.g. reiterated the unfortunate distinction between norms and rules, paras. 15–68, and international law, paras. 69–73.

97 The UN OEWG Final Report dedicates only four out of 80 paragraphs to the application international law in cyberspace and even these paragraphs remain very general, paras. 34–37.

98 Microsoft, Five Principles for Shaping Cybersecurity Norms, 2013; Microsoft, International Cybersecurity Norms – Reducing conflict in an Internet-dependent world, 2014; Microsoft, From Articulation to Implementation: Enabling progress on cybersecurity norms, 2016.

99 Global Commission on the Stability of Cyberspace, 'Advancing Cyberstability', Final Report, November 2019, Annex B.

100 Schmitt, 'Tallinn Manual on Cyber Warfare' 2013 (n. 17); Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1).

2020 it was announced that a third Tallinn Manual would follow.[101] Such proposals as expert or stakeholder manuals evidently lack legal authority[102] but in particular the Tallinn Manual has been remarkably successful in influencing the international legal discourse and is cited by various states in their statements on international law in cyberspace.[103] Due to this influence in particular the Tallinn Manual plays an important role for this study and is cited at various points. Yet, it is important to be mindful of its lack of legal authority.

IV. Turn to preventive approaches against cyber security risks

As a way forward states have increasingly turned to preventive approaches which bypass the notorious challenges of reactive approaches in cyberspace and focus on cyber resilience to better identify, protect against, respond to

101 NATO CCDCOE, 'CCDCOE To Host the Tallinn Manual 3.0 process', 14 December 2020, https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/; the CCDCOE has furthermore published the Cyber Law Toolkit 2024, an interactive resource on international law and cyber operations, available at: https://cyberlaw.ccdcoe.org/wiki/Main_Page.

102 Cautioning against expert manuals as authoritative documents in international law Anton Petrov, *Expert Laws of War Restating and Making Law in Expert Processes* (Cheltenham et al.: Edward Elgar 2020); see also critically of the methodology of the Tallinn Manual 1 anticipating crises and narratives and potential repercussions for other areas of international law, Heike Krieger, 'Conceptualizing Cyberwar, Changing the Law by Imagining Extreme Conditions?', in Thomas Eger/Stefan Oeter/Stefan Voigt (eds), *International Law and the Rule of Law under Extreme Conditions: An Economic Perspective* (Tübingen: Mohr Siebeck 2017), 195–212, at 201; on the risk of undermining the legal legitimacy of the proposed rules see Heike Krieger/Jonas Püschmann, 'Law-making and legitimacy in international humanitarian law', in Heike Krieger (ed.), *Law-Making and Legitimacy in International Humanitarian Law* (Cheltenham et al.: Edward Elgar 2021), 1–14, at 8. The Tallinn Manual itself acknowledges its lack of legal authority Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), p. 2: 'It is essential to understand that Tallinn Manual 2.0 is not an official document, but rather the product of two separate endeavours undertaken by groups of independent experts (…) The Manual does not represent the views of the NATO CCD COE, its sponsoring nations, or NATO. Nor does it reflect the position of any other organisation or State represented by observers or of any of the States involved in the 'Hague Process' (…) Ultimately, Tallinn Manual 2.0 must be understood only as an expression of the opinions of the two International Groups of Experts as to the state of the law'.

103 See e.g Netherlands, 'International Law in Cyberspace' 2019 (n. 89) p. 3; Germany, 'Application of International Law' 2021 (n. 90), p. 2.

and recover from cyber threats.[104] E.g. France has alluded to the advantages of preventive approaches in light of notorious attribution problems.[105] The European Union (EU) has made prevention and resilience one of the central aspects of its cyber strategy.[106] The need for cooperative prevention of cyber harm is also mentioned in a Memorandum of Understanding (MoU) between the EU and the Association of Southeast Asian Nations (ASEAN)[107], as well as by the Non-Aligned Movement (NAM).[108] States increasingly acknowledge that often the most effective risk mitigation is prevention and resilience instead of retaliation.[109] For implementing preventive approaches in cyberspace the harm prevention rule takes centre stage.

104 *Microfocus,* 'What is Cyber Resilience', available at: https://www.microfocus.com/en-us/what-is/cyber-resilience; Underlining the importance of resilience also ILA, 'Cybersecurity and Terrorism' 2016 (n. 10), p. 70, para. 245.

105 France, 'Strategic Review' 2018 (n. 29), p. 9: 'The uncertainty intrinsically linked to the attribution of an attack should encourage states to focus their efforts on preventive measures.'

106 EU, Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, 16 December 2020, p. 4f.

107 ASEAN-EU Statement on Cybersecurity Cooperation, 1 August 2019, para.4.

108 NAM Working Paper for the Second Substantive Session of the Open-ended Working Group on developments in the Field of Information and Telecommunications in the Context of International Security (UN OEWG), para. 19: 'States should focus on cooperating to prevent conflicts in cyberspace from erupting in the first place.'

109 The Tallinn Manual has also recognized that in cyberspace an act of mitigation is often less effective than its prevention, see Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 7, p. 46, para. 11: '[I]n light of the nature of cyber activities, preventive measures are arguably prudent. For instance, the speed of cyber operations often makes an act of mitigation less effective than the successful prevention thereof'; on the inferiority of reaction to prevention in the environmental context Jutta Brunnée, 'Procedure and Substance in International Environmental Law', *Recueil des Cours de l'Académie de Droit International de la Haye* 405 (2020) 77–240, at 158: '[I]t is plain that prevention is what is needed, since "reaction" is generally inferior, and sometimes impossible.'

Chapter 2: The Harm Prevention Rule in International Law

A. The harm prevention rule in international law

The harm prevention rule expresses the rationale that a state has to prevent harm from known risks to the legally protected interests of other states that emanate from its territory or under its control. The origins of this rationale can be traced back to the writings of Grotius, Pufendorf, Hall and Oppenheim.[1] The rationale that a legal entity that exercises control over risky activities may be held accountable for controlling this risk can also be found in various domestic tort laws.[2] In international law, due to the centrality of the state which exercises sovereignty over its territorial boundaries, it is presumed that the state is in the best position to control risks emanating from its territory. This presumption and rationale has been asserted in a string of cases in international legal proceedings.

I. The evolution of the harm prevention rule in international law

The first instance was the *Alabama* arbitration in 1871 between the US and the UK. In this case, the arbitral tribunal held the UK responsible for its failure to detain vessels in British shipyards which were later used for attacks against merchant ships in the US Civil War. The tribunal found that Britain had violated its due diligence duties under the law of neutrality

1 On the concept of patienta proposed by Grotius based on which responsibility would arise if a sovereign knew of a crime to be committed by an individual in its territory, as well as Pufendorf's suggestion to presume that the state could have prevented harmful private conduct and presumed responsibility as a consequence see Maria Monnheimer, *Due Diligence Obligations in International Human Rights Law* (Cambridge: Cambridge University Press 2021) 80f.; on the historical roots of due diligence in international law see also Giulio Bartolini, 'The Historical Roots of the Due Diligence Standard', in Heike Krieger/Anne Peters/Leonhard Kreuzer (eds.), *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 23–41.

2 Elspeth Reid, 'Liability for Dangerous Activities: A Comparative Analysis', *International Comparative Law Quarterly* 48 (1999), 731–756, at 755.

'to take (…) effective measures of prevention'.[3] Several years later, the US Supreme Court asserted the rationale in a broad manner beyond the law of neutrality in the *Arjona* case, asserting that in principle any kind of harm to other states' legally protected interests would need to be prevented by the territorial state. It asserted:

> 'The law of nations requires every national government to use "due diligence" to prevent a wrong being done within its own dominion to another nation with which it is at peace, or to the people thereof'[4]

The broad reference to any kind of 'wrong' indicates the holistic protection of other states' legal interests under the rule. This holistic protection was subsequently reiterated by arbitrator *Max Huber* in the *Island of Palmas* case who broadly referred to a state's duty to protect the *rights* of other states within its territory:

> 'Territorial sovereignty (…) involves the exclusive right to display the activities of a State. The right has as corollary a duty: the obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability (…).'[5]

Subsequently, the *Trail Smelter* Arbitration and the *Corfu Channel* case – probably the two most-cited cases on the harm prevention rule – affirmed the rule's general cross-sectoral dimension. The *Trail Smelter* arbitration of 1941 between the US and Canada dealt with a zinc smelter at the border between Canada and the USA. This smelter caused injury to US territory through the emission of fumes. The Tribunal held:

> 'The Tribunal, therefore, finds (…) that, under the principles of international law (…) no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein (…).'[6]

3 *Alabama Claims of the United States of America against Great Britain*, Award of 14 September 1872, UNRIAA, vol. XXIX, 129.
4 US Supreme Court, *United States v. Arjona*, 7 March 1887, 120 U.S. Reports 1887, 484.
5 Arbitrator Max Huber, *Island of Palmas Case (Netherlands v. United States of America),* Award of 4 April 1928, PCA Case No. 1925–01, p. 9, Vol. II, p. 829 at p. 839.
6 *Trail Smelter Case (United States v. Canada)*, Decisions of 16 April 1938 and 11 March 1941, vol. III, UNRIAA, 1905–1982, at 1965.

In line with the above-mentioned decisions the tribunal did not limit its assertion to transboundary harm but referred to protection against 'injurious acts', hereby expressing the cross-sectoral dimension[7] of the rationale:

> '[A] state owes at all times a duty to protect other States against injurious acts by individuals from within its jurisdiction.'[8]

In the *Corfu Channel* case the International Court of Justice (ICJ) asserted the same rationale similarly broadly. Albania had failed to warn British ships in its territorial sea about mines laid there. The mines exploded and severely damaged British warships. Employing the general reference to 'rights' of other states reminiscent of the *Island of Palmas* dictum the ICJ asserted

> 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.'[9]

The same harm prevention rationale was later reiterated by the ICJ in its Advisory Opinion in *Nuclear Weapons*[10], *Pulp Mills*[11], *Certain Activities*[12] and with regard to physical transboundary harm by the ILC in its Draft Articles on the Prevention of Transboundary Harm.[13]

---

7 Pierre-Marie Dupuy/Cristina Hoss, 'Trail Smelter and Terrorism: International Mechanism to Combat Transboundary Harm', in Rebecca M. Bratspies/Russell A. Miller (eds.), *Transboundary Harm in International Law: Lessons from the Trail Smelter Arbitration* (Cambridge: Cambridge University Press 2006), 225–239.

8 'Trail Smelter' (n. 6), 1963.

9 ICJ, *Corfu Channel Case (United Kingdom v. Albania)*, Judgment of 9 April 1949, ICJ Reports 1949, 4, p. 22.

10 ICJ, *Legality of the Threat or Use of Nuclear Weapon*s, Advisory Opinion of 8 July 1996, ICJ Reports 1996, 226, para. 241.

11 ICJ, *Pulp Mills on the River Uruguay Case (Argentina v. Uruguay)*, Judgment of 20 April 2010, ICJ Reports 2010, p. 14, 45, para. 101.

12 ICJ, *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua), Construction of a Road in Costa Rica along the River San Juan (Nicaragua v. Costa Rica)*, Judgment of 16 December 2015, ICJ Reports 2015, p. 665, para. 104.

13 United Nations, International Law Commission (ILC), Draft Articles on the Prevention of Transboundary Harm from Hazardous Activities, A/RES/56/82, 12 December 2001; the Draft Prevention articles (as well as the the principles on the allocation of loss in the case of transboundary harm arising out of hazardous activities, annexed to UN General Assembly Resolution A/RES/61/36) have been repeatedly commended by the UN General Assembly but have not been adopted by states yet: UN General Assembly Resolution A/RES/74/189, 30 December 2019, paras. 1–5.

II. Holistic protection of interests of other states

Often the protection of territorial sovereignty and integrity is highlighted[14] as the main protected legal good under the harm prevention rule. Yet, the above-mentioned cases show that legally protected interests of states are also protected holistically beyond their territory. Already in the *Corfu Channel* case harm occurred extraterritorially: The UK warship was harmed in the Albanian territorial sea and therefore outside of British territory. Also the *Tehran Hostages* case concerned diplomatic premises seized by non-state actors on the territory of another than the affected state.[15] In the *Neer* case, the Mexico-US General Claims Commission also found a violation of a state's rights under the rule although harm occurred outside of the territory of the violated state.[16] That the harm prevention rule extends beyond the protection of territorial integrity can also be seen in international economic law which evades the territorial-extraterritorial dichotomy due to the non-tangibility of economic harm.[17] Due to this broad protective scope the harm prevention rule is linked not only to the protection of territorial integrity, but also to sovereign equality[18], non-interference[19], and

14 ILC Special Rapporteur Julio Barboza, 'International Liability for the Injurious Consequences of Acts Not Prohibited by International Law and Protection of the Environment', *Recueil des Cours de l'Academie de Haye* 247 (1998), 291–406, at 330: '(…) causing transboundary harm is contrary to the well-established right of territorial sovereignty of States.'

15 ICJ, *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgment of 24 May 1980, ICJ Reports 1980, p. 3, 33, para. 68.

16 Mexico-US General Claims Commission, *L. F. H. Neer and Pauline Neer (USA v. United Mexican States)*, 15 October 1926, vol. IV, UNRIAA, 62, para. 4.

17 Markus Krajewski, 'Due Diligence in International Trade Law', in Krieger/Peters/Kreuzer, 'Due Diligence' 2020 (n. 1), 312–328, at. 312; Jelena Bäumler, 'Implementing the No Harm Principle in International Economic Law: A Comparison between Measure-Based Rules and Effect-Based Rules', *Journal of International Economic Law* 20 (2017), 807–828.

18 See linking the harm prevention rule to sovereign equality ICJ, *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua), Construction of a Road in Costa Rica along the River San Juan (Nicaragua v. Costa Rica)*, Separate Opinion of Judge Donoghue, ICJ Reports 2015, p. 784, para. 8: '[T]aking into account the sovereign equality and territorial sovereignty of States, it can be said that, under customary international law, a State of origin has a right to engage in activities within its own territory, as well as an obligation to exercise due diligence in preventing significant transboundary environmental harm'.

19 ILA Study Group on Due Diligence in International Law, Second Report, July 2016, p. 5.

the international rule of law.[20] This broad protective scope of the rule beyond territorial integrity is particularly valuable in cyberspace: Cyber harm is often non-physical and can occur wholly ICT-internal, without tangible physical harm affecting the territorial integrity of another state.[21]

III. Territory, jurisdiction or control: Risk proximity as basis of accountability

The scope of the duty to exercise due diligence to prevent significant harm applies to activities that occur on the territory of a state, under its jurisdiction or under its control.[22] Decisive for all three concepts is risk proximity[23] and the ability or power[24] to influence potentially harmful or risky behaviour. The primary basis for due diligence obligations – also in cyberspace – is the principle of territoriality. In this regard it becomes relevant that the principle of territorial sovereignty applies in cyberspace.[25] As states have jurisdiction over the physical layer of cyberspace on their

20 Also linking the harm prevention rule reference in the UN GGE Reports to the rule of law Enekken Tikk/Mika Kerttunen, 'The Alleged Demise of the UN GGE: An Autopsy and Eulogy', *Cyber Policy Institute,* 2017, p. 35.

21 See chapter 1.C; also arguing that focus on territorial integrity is unfit to assess cyber harm Harriet Moynihan, 'The Application of International Law to State Cyberattacks Sovereignty and Non-intervention', *Chatham House – Research Paper*, 2019, fn. 102.

22 ICJ, Legality of Nuclear Weapons Opinion (n. 10), para. 29: 'The existence of the general obligation of States to ensure that activities *within their jurisdiction and control* respect the environment of other States or of areas beyond national control is now part of the corpus of international law relating to the environment'; Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press 2017), rule 6: 'A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.'

23 Federica Violi, 'The Function of the Triad "Territory", "Jurisdiction", and "Control" in Due Diligence Obligations', in Krieger/Peters/Kreuzer, 'Due Diligence' 2020 (n. 1), 75–91, at 91.

24 For the context of human rights Marko Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (Oxford: Oxford University Press 2011), 40, 41: 'Jurisdiction', in this context, simply means actual power, whether exercised lawfully or not—nothing more, and nothing less.'

25 United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), A/70/174, 22 July 2015 (UN GGE Report 2015), para. 28a; United Nations, Report of the Group of Governmental Experts on Advancing Responsible

territory (i.e. fibre-optic cables, routers, servers and individuals using cyberspace), they are in the position to control or influence risky cyber activities emanating from this physical layer. That the ICT infrastructure is de-centralised and primarily privately owned and operated does not affect the existence of states' territorial jurisdiction. As noted by ICJ Judge *Tomka* in his Declaration in the *Uganda/DRC* case, the fact that a state only exercises limited control over certain areas of its territory does not free it from its vigilance or diligence duties.[26] Various potential procedural due diligence obligations for harm prevention, such as duties to assist or mitigate[27] may in fact require that states gain control over cyber activities, e.g. by forcing private ICT operators to interrupt data flows, by enforceing such an order themselves, or by accessing and preserving computer data for securing evidence in criminal investigations.[28] Also the limited control of states through which data only transits does not free such states from due diligence obligations as they also in principle have the capacity to influence such activities transiting their territory.[29]

It is worth noting that the function of the triad 'territory, jurisdiction, control' under the harm prevention rule thereby deviates from the primary function of jurisdiction as a *right*. Jurisdiction in general international law generally denotes a state's right to make and enforce rules to regulate activities.[30] By contrast, in the context of the harm prevention rule, jurisdiction

State Behaviour in Cyberspace in the Context of International Security (UN GGE), A/76/135, 14 July 2021 (UN GGE Report 2021), para. 71b; see also chapter I.D.II.

26 ICJ, *Case Concerning Armed Activities on the Territory of the Congo (DRC v. Uganda)*, Declaration of Judge Tomka, ICJ Reports 2005, p. 352, para. 4: 'The geomorphological features or size of the territory does not relieve a State of its duty of vigilance nor render it less strict. Nor does the absence of central governmental presence in certain areas of a State's territory set aside the duty of vigilance for a State in relation to those areas.'

27 On a duty to take action against imminent or ongoing harm as a due diligence requirement see chapter 4.C.II.

28 On criminal procedural measures as a due diligence requirement see chapter 4.D.I.5.

29 See also UN GGE Report 2021, para. 29: 'This norm reflects an expectation that if a State is aware of or is notified in good faith that an internationally wrongful act conducted using ICTs is emanating from or transiting through its territory it will take all appropriate and reasonably available and feasible steps (…)'.

30 Bernard H. Oxman, 'Jurisdiction of States', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2007), para. 1: 'In its broadest sense, the jurisdiction of a State may refer to its lawful power to act and hence to its power to decide whether and, if so, how to act, whether by legislative, executive, or judicial means'. The right to exclusive regulatory and enforcement jurisdiction is a core right derived from sovereignty, see James Crawford,

and control create accountability by requiring a state to exercise due diligence against risks of harm. Hereby, jurisdiction is transformed from a right to a duty.[31] The manifold discussions on jurisdictional clashes and conflicts that frequently occur in cyberspace, e.g. with regard to regulation of search engines or in the area of data protection[32] are only insofar relevant for the harm prevention rule as the exercise of jurisdiction (as a right) creates risk proximity (and consequently due diligence obligations to prevent).

IV. Knowledge of risk of harm required

Under the harm prevention rule states are not held liable for every harmful activity emanating from their territory. They need to have knowledge of the harmful activity.[33] If the occurrence of harm is unpredictable a state is not held accountable for not taking diligence measures against it. It is not necessary that a state actually knew of a harmful activity. In the *Corfu Channel* case the ICJ e.g. held Albania accountable although it was not known whether Albania actually knew of a risk of harm.[34] It was sufficient that, under the specific circumstances, it ought to have known. Hence, so-called constructive knowledge suffices to trigger due diligence-based accountability under the harm prevention rule.[35] The question what a state 'ought to have known' in cyberspace is a highly complex question that depends on the level of control a state can and should exercise over internet traffic routes, traffic and content data in cyberspace.[36]

Brownlie's Principles of Public International Law (Oxford: Oxford University Press 2019), 432.

31 On jurisdiction as an obligation with regard to universal criminal jurisdiction Alex Mills, 'Rethinking Jurisdiction in International Law', *British Yearbook of International Law* 84 (2014), 187–239, at 210.

32 See Uta Kohl, 'Jurisdiction in Cyberspace', in Nicholas Tsagourias/Russell Buchan (eds.) *Research Handbook on International Law and Cyberspace (Cheltenham:* Edward Elgar Publishing 2015), 30–54; on jurisdictional competences in cyberspace Schmitt, 'Tallinn Manual 2.0' 2017 (n. 22), commentary to rules 8–13, p. 51–78.

33 See ICJ, 'Corfu Channel' (n. 9), p. 22: Bartolini, 'Historical Roots' 2020 (n. 1), 38; Jason D. Jolley, *Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law* (University of Glasgow 2017), paras. 23ff.

34 ICJ, 'Corfu Channel' (n. 9), p. 22.

35 See in more detail on actual and constructive knowledge in cyberspace and potential due diligence duties to acquire knowledge chapter 4.D.II.

36 In more detail on what states are expected to know about harmful cyber activities on their territory or jurisdiction ibid.

V. The duty to exercise due diligence to prevent and mitigate harm

As a consequence of knowledge about a harmful activity and the capacity to influence it the harm prevention rule requires states to exercise due diligence to prevent and mitigate harm emanating from their territory (or jurisdiction or control).

1. Due diligence as an obligation of conduct

Regarding the required standard of conduct, the commentaries to the ILC Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, adopted in 2001, exemplarily highlight the most important legal aspects regarding compliance with due diligence:

> 'The obligation of the State of origin to take preventive or minimization measures is one of due diligence (…) The duty of due diligence (…) is not intended to guarantee that significant harm be totally prevented, if it is not possible to do so. In that eventuality, the State … [must] exert its best possible efforts to minimize the risk. In this sense, it does not guarantee that the harm would not occur.'[37]

The duty to exercise due diligence to prevent harm is hence an obligation of conduct and does not lead to strict liability.[38] States are merely required to exercise best efforts, to use 'all appropriate measures'[39] to prevent harm which are reasonable under the respective circumstances. If

37 ILC, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, UN General Assembly Resolution A/RES/56/10, 23 April-1 June, 2 July-10 August 2001, commentary to art. 3, p. 154, para. 7.

38 On due diligence as a modality Anne Peters/Heike Krieger/Leonhard Kreuzer, 'Dissecting the Leitmotif of Current Accountability Debates: Due Diligence in the International Legal Order', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 1–19, at 2: 'Due diligence thus is no free-standing obligation but a modality attached to a duty of care for someone or something else (including the duty to prevent and mitigate harm). One might call it an ancillary obligation if one wants to use the language of obligation at all.'

39 ILC, 'Draft Articles on Prevention' 2001 (n.37).

harm nevertheless occurs they are not held liable.[40] Concerning cyberspace, the UN GGE Report 2021 referred to the duty to take 'appropriate and reasonably available and feasible steps'.[41] The open-ended flexibility of the due diligence standard based on context-dependent appropriateness and reasonability make it a particularly attractive tool for cyberspace: If a certain standard of diligence is beyond a state's capacity, e.g. due to limited economic or technical resources, the state is not held liable.[42] The capacity-dependent interpretation of the required standard of due diligence hence avoids overburdening states. Regarding the greatly diverging technological ICT capacities of states this aspect is particularly relevant in cyberspace. Only with regard to some measures an objective minimum standard regardless of capacity must be fulfilled.[43]

Despite its context-dependent flexibility the duty to exercise due diligence under the harm prevention rule is a binding obligation. Lack of

40 ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment of 26 February 2007, ICJ Reports 2007, p. 43, para. 430.

41 UN GGE Report 2021, para. 29. 'This norm reflects an expectation that if a State is aware of or is notified in good faith that an internationally wrongful act conducted using ICTs is emanating from or transiting through its territory it will take all appropriate and reasonably available and feasible steps to detect, investigate and address the situation.'

42 ILA, Second Report 2016 (n. 19), 2016, p. 3: 'Due diligence introduces flexibility in this respect to serve a broader international community objective to ensure that States with limited economic capacity can participate in the international legal system without being burdened by unreasonable normative demands'; implicitly affirming the relevance of a state's capacity for discharging the duty to prevent ICJ, *Tehran Hostages* (n.15), para. 63.

43 ILC, 'Draft Articles on Prevention' 2001 (n. 37), commentaries to art. 3, p. 155, para. 17: 'It is, however, understood that the degree of care expected of a State with a well-developed economy and human and material resources and with highly evolved systems and structures of governance is different from States which are not so well placed. Even in the latter case, vigilance, employment of infrastructure and monitoring of hazardous activities in the territory of the State, which is a natural attribute of any Government, are expected'; see also Mexico-US General Claims Commission, *L. F. H. Neer and Pauline Neer (USA v. United Mexican States)*, 15 October 1926, vol. IV, UNRIAA, 60, para. 4: '[the] treatment of an alien, in order to constitute an international delinquency, should amount to an outrage, to bad faith, to wilful neglect of duty, or to an insufficiency of governmental action so far short of international standards that every reasonable and impartial man would readily recognize its insufficiency. Whether the insufficiency proceeds from deficient execution of an intelligent law or from the fact that the laws of the country do not empower the authorities to measure up to international standards is immaterial.'

diligence – i.e. negligence – hence leads to state responsibility.[44] In this regard it is important to note that due diligence under the harm prevention rule is distinct from due diligence as a non-binding standard of conduct, for example with regard to UN Peacekeeping, where it functions as a non-binding soft standard of conduct for 'doing' due diligence, inter alia in the context of voluntary risk evaluation[45], or in the context of business and human rights in which it has – at least on the international legal level – predominantly been discussed as a non-binding operational principle for businesses to address their human rights impact.[46]

2. The preventive and remedial dimension of due diligence

Due diligence for harm prevention may require preventive acts before, during and after harmful incidents. This extended temporal dimension of due diligence was already expressed in the *Trail Smelter* arbitration which referred to the duty to protect 'at all times'. It is important to highlight the extended temporal dimension under the harm prevention rule as the Tallinn Manual rejected a preventive dimension of due diligence and asserted that it merely requires to 'stop' ongoing harm.[47] Such a reduction of due diligence to merely 'stop' harm, however, seems hard to square with

44 See below chapter 5.B.

45 Neil McDonald, 'The Role of Due Diligence in International Law', *International and Comparative Law Quarterly* 68 (2019), 1041–1054, at 1042; Anne Peters/Heike Krieger/Leonhard Kreuzer, 'Due diligence: the risky risk management tool in international law', *Cambridge Journal of International Law* 9 (2020), 121–136, at 133.

46 In this context, the so-called 'Ruggie Principles'; proposed by UN Special Representative John Ruggie and endorsed by the UN Human Rights Council, have played an important role. See Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, A/HRC/17/31, 21 March 2011, para. 17. While a UN Intergovernmental Working Group has been working on a legally binding treaty on mandatory human rights due diligence of businesses since 2014 so far only on the domestic and regional level binding obligations on businesses' human rights due diligence exist, see e.g. section 3 of the German Supply Chain Act which entered into force in 2023 or the EU Corporate Sustainability Due Diligence Directive adopted by the European parliament in April 2024 and approved by the Council of the European Union in May 2024, Directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859, arts. 5f.

47 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 22), commentary to rule 7, p. 45, para. 7: 'In other words, the term 'prevent' in this context means 'stop''.

the holistic risk mitigation rationale of the harm prevention rule.[48] Already the *Corfu Channel* case gives evidence that due diligence may also require preventive measures before the moment of imminent or occurring harm. In the case, the ICJ held Albania responsible for its failure to take preventive measures:

> 'In fact, nothing was attempted by the Albanian authorities to prevent the disaster. These grave omissions involve the international responsibility of Albania.'[49]

Also in the *Trail Smelter* case the tribunal directed the installation of preventive control measures, such as sulphur dioxide records, to control risky activities and prevent future harm[50], hereby underscoring the extended temporal dimension.[51] Exercising due diligence is hence a largely continuous obligation that does not only live up temporarily but needs to be exercised 'at all times'.[52]

VI. The negative prohibitive dimension of the harm prevention rule

Due to the focus of the harm prevention rule on due diligence for harm prevention it is often neglected that the harm prevention rule also entails a negative prohibitive dimension. This follows from an argument *a fortiori*. If a state is already obliged to prevent harmful activities that are not attributable to it then even more it must be obliged not to conduct such harmful activities itself. The Tribunal noted this negative prohibitive dimension in *Trail Smelter*:

> 'The Tribunal, therefore, finds (…) that, under the principles of international law (…) no State has the right to use or permit the use of its

48 Also critical of the restrictive stance of the Tallinn Manual Talita de Souza Dias/Antonio Coco, *Cyber Due Diligence in International Law* (Print version: Oxford Institute for Ethics, Law and Armed Conflict 2021), 165.

49 ICJ, 'Corfu Channel' (n. 9), p. 23.

50 'Trail Smelter' (n. 6), 1966: '(…) in order to avoid damage occurring, the Tribunal now decides that a régime or measure of control shall be applied to the operations of the Smelter and shall remain in full force (…)'.

51 See in more detail on the anticipatory dimension of due diligence that requires measures also with regard to abstract or general risks chapter 3.A.I.

52 'Trail Smelter' (n. 6), 1963.

> territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein (…).'[53]

The Tribunal's assertion that no state has the right to '*use*' its territory in a harmful way indicates that the harm prevention rule can also be violated by active acts of a state. Also the assertion of ILC Special Rapporteur *Barboza* – integrating both the *Trail Smelter* and *Corfu Channel* dicta – reflects this negative prohibitive dimension of the harm prevention rule:

> '(…) there is a general prohibition of 'knowingly' using or permitting the use of a State's territory contrary to the rights of other States, as the Corfu Channel decision very rightly established – and before that did the Tribunal of the Trail Smelter Case – and that causing transboundary harm is contrary to the well-established right of territorial sovereignty of States.'[54]

Commentators have highlighted the negative prohibitive dimension of the harm prevention rule in other areas of international law[55], as well as in cyberspace.[56] Also the Tallinn Manual implicitly acknowledges that the harm prevention rule also applies to acts of states.[57] The negative prohibitive dimension may also be read into para. 28 lit. e of the UN GGE Report 2015 which asserts that states 'must not use proxies' to commit internationally wrongful acts. Although acts of proxies are not necessarily acts of a state or attributable to it, the phrasing of the first half of para. 28 lit. e suggests that the norm aims at constraining malicious state behaviour.[58] New Zealand asserted the negative prohibitive dimension even explicitly:

---

53 Ibid., 1965.

54 Barboza, 'International Liability' 1998 (n. 14), at 330.

55 Jelena Bäumler, *Das Schädigungsverbot im Völkerrecht* (Berlin: Springer 2017), 1: 'Der Grundsatz sic utere tuo ut alienum non laedas besagt, dass niemand seine Rechte so nutzen soll, dass einem anderen Schaden entsteht. Es ist also das Verbot, einen anderen zu schädigen'.

56 Coco/Dias, 'Cyber Due Diligence Report' 2021 (n. 48), 65.

57 See chapter 4.A; Schmitt, 'Tallinn Manual 2.0' 2017 (n. 22), commentary to rule 6, p. 33, para. 12: 'Attachment of the due diligence obligation extraterritorially clearly occurs when a State exercises exclusive control over particular cyber infrastructure or activities. In cases of concurrent control by more than one State, both States bear the obligation of due diligence. An example would be a cyber operations facility run jointly by two States.'

58 It distinguishes acts of proxies from acts of non-state actors, hereby suggesting state proximity UN GGE Report 2015, para. 28 lit. e: 'States must not use proxies to

> 'Bearing those factors in mind, and having regard to developing state practice, New Zealand considers that territorial sovereignty prohibits states from using cyber means to cause significant harmful effects manifesting on the territory of another state'[59]

The contrary logic that below the threshold of an intervention states are uninhibited by international law in their actions as long as no prohibitive rule exists is reminiscent of the notorious *Lotus* doctrine – seemingly underlying some states' statements[60] – which has however repeatedly been discarded.[61]

commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts'.

59 New Zealand, The Application of International Law to State Activity in Cyberspace, 1 December 2020, para. 14.

60 See with regard to a potential prohibitive sovereignty rule UK Attorney General Wright, Cyber and International Law in the 21st Century, Speech 23 May 2018: 'I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention'; Paul C. Ney, Department of Defense General Counsel Remarks at U.S. Cyber Command Legal Conference, Speech of 2 March 2020: 'For cyber operations that would not constitute a prohibited intervention or use-of-force, the Department believes there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's territory.'

61 ICJ Judge Simma has described it as an 'old, tired view of international law' ICJ, *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo*, Declaration of Judge Simma, p. 478, para.2; An Hertogen, 'Letting Lotus Bloom', *European Journal of International Law* 26 (2015), 901–926, at 912: 'This residual rule is not freedom to act but, rather, the idea that territorial sovereignty deserves protection to ensure the co-existence of independent communities and facilitate the achievement of common aims. Only if an action does not jeopardize these goals will states be free to act.'; ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Dissenting Opinion Judge Shahabuddeen, ICJ Reports 1996, p. 375, 393–394: 'Thus, however far-reaching may be the rights conferred by sovereignty, those rights cannot extend beyond the framework within which sovereignty itself exists; (…) It is difficult for the Court to uphold a proposition that, absent a prohibition, a State has a right in law to act in ways which could deprive the sovereignty of all other States of meaning'.

B. The harm prevention rule as the most suitable term for expressing the due diligence rationale

Despite the rule's long history in international judicial proceedings, treaties and state practice precision regarding the terminology and doctrinal character of the rule is often neglected in the international legal discourse. Some commentators refer to rule as the 'obligation' or the 'principle' of due diligence.[62] Others refer to the *sic utere tuo* principle.[63] Again others to the 'no harm rule' or to the 'duty to prevent harm'[64], or avoid labelling the rule altogether. The ICJ in *Pulp Mills* neutrally referred to the due diligence that 'is a required of a state in its territory'.[65]

Which terminology is chosen does not seem to be based on a consistent logic. While references to the 'no harm rule' are particularly prominent in international environmental law, the 'no harm rule' is also referenced in international economic law.[66] The *Corfu Channel* is a prominent reference point both for the 'obligation' or 'principle' of due diligence, as well as for the 'no harm rule'.[67] Also the *Trail Smelter* is a frequent reference for

62 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 22), commentary to rule 6, p. 31, 32:' The due diligence principle is sometimes also referred to as the 'obligation of vigilance', the 'obligation of prevention', or the 'duty of prevention'. The International Group of Experts adopted the term 'due diligence' in light of its prevalent use, but concurred that it can be regarded as synonymous with the term 'obligation of vigilance'.

63 Bäumler, 'Schädigungsverbot' 2017 (n. 55), 1.

64 On the interchangeable use of the term see Antonio Coco/Talita de Souza Dias, ''Cyber Due Diligence': A Patchwork of Protective Obligations in International Law', *European Journal of International Law* 32 (2021), 771–805, at 775, 776; Katharina Ziolkowski, 'General Principles of International Law as Applicable in Cyberspace' in Katharina Ziolkowski (ed.) *Peacetime Regime for State Activities in Cyberspace* (NATO CCDCOE 2013), 135–188, at 165.

65 ICJ, 'Pulp Mills', 2010 (n. 11), para. 101: 'The Court points out that the principle of prevention, as a customary rule, has its origins in the due diligence that is required of a State in its territory.'

66 Bäumler, 'Schädigungsverbot' 2017 (n. 55), 1.

67 Bäumler, 'Schädigungsverbot' 2017 (n. 55), 1; Jutta Brunnée, 'Procedure and Substance in International Environmental Law', *Recueil des Cours de l'Académie de Droit International de la Haye* 405 (2020) 77–240, at 126; Karine Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations', *Baltic Yearbook of International Law* 14 (2014), 23–39, at 25; Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', *Journal of Conflict & Security Law* 21 (2016), 429–453, at 440.

what commentators refer to as the obligation or rule of 'due diligence'.[68] The ILC in its Prevention Articles asserted the 'duty to prevent significant transboundary harm' but did not elaborate the choice of terminology.[69] Overall, the mix of divergent formulations reflects the gradual evolution of the rule and potential sector-specific nuances. Yet, due to the connecting line between the *Alabama, Island of Palmas, Trail Smelter* and *Corfu Channel* the divergent references are unsatisfactory. No terminology is clearly preferable over another and a certain degree of misunderstanding in the international legal discourse seems inevitable.

Perhaps the most prominent terminology used for the rule is to refer to it as an obligation of due diligence. Yet, such a reference risks to cause misunderstanding. Beyond the rationale expressed in *Corfu Channel* and the above-mentioned other cases due diligence is a standard of conduct for *soft law* responsibilities and informal 'doing diligence' expectations in international law. It is e.g. prominently discussed in the context of corporate social responsibility discourses on business and human rights.[70] Furthermore, due diligence is not an autonomous primary rule on its own. Due diligence does not have an intrinsic, self-ascertainable content.[71] It is a standard of conduct whose content is determined by an aim which is determined by a *distinct* primary rule.[72] Even in its most basic form – the harm prevention rule – its content is determined in relation to the target of preventing significant harm. To assert a self-standing 'due diligence obligation' hence has several disadvantages.

68 Sarah Heathcote, 'State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility', in Karine Bannelier/Theodore Christakis/Sarah Heathcote (eds.), *The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case* (London et al.: Routledge 2012), 295–314, at 297, 298; Eric Talbot Jensen/Sean Watts, 'Due Diligence and the US Defend Forward Cyber Strategy', *Aegis Series Paper No. 2006*, p. 10.

69 ILC, 'Draft Articles on Prevention' 2001 (n.37), commentary to art. 3, p. 153, para. 3.

70 See already above chapter 2.A.V.1; on the link between human rights protection, compliance and economic self-interests of businesses in this context see Björnstjern Baade, 'Due Diligence and the Duty to Protect Human Rights', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 92–108, at 95.

71 Bäumler, 'Schädigungsverbot' 2017 (n. 55), 293.

72 Heike Krieger/Anne Peters, 'Due Diligence and Structural Change in the International Legal Order', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 351–390, at 375.

To refer to it as a 'principle of due diligence' would seem to suggest that due diligence is a general principle of international law – yet, its characterization as a general principle is best avoided as it would distract that due diligence always needs to a primary rule to ascertain its content.[73]

To alternatively refer to the 'no harm rule' seems to suggest that the rule's rationale stipulates an obligation of result that *no* harm occurs. Yet, this would be misleading as the duty to exercise due diligence to prevent harm is an obligation of conduct. Furthermore, asserting a 'no harm rule' does not reflect the preventive dimension of the rule. While assertions of the 'no harm' rule reflect the evolution of the rule in cases in which harm had occurred and are hence plausible with regard to specific cases, such as e.g. the *Trail Smelter* case, it is preferable not to use the label 'no harm' rule.

Other commentators have named the rule after leading cases and e.g. asserted a 'Corfu Channel rule' and a 'Trail Smelter rule'.[74] However, the introduction of a distinction between a '*Corfu Channel* rule' and a '*Trail Smelter rule*' seems unnecessary. That *Trail Smelter* and *Corfu Channel* cases express the same legal rationale is expressed by ILC Special Rapporteur *Barboza:*

> 'The former evidence seems to indicate that there is a general prohibition of "knowingly" using or permitting the use of a State's territory contrary to the rights of other States, as the Corfu Channel decision very rightly established – and before that did the Tribunal of the Trail Smelter Case – and that causing transboundary harm is contrary to the well-established right of territorial sovereignty of States.'[75]

It was argued that the main difference between *Trail Smelter* and *Corfu Channel* is that *Trail Smelter* establishes liability for lawful acts – the 'liability regime' – while *Corfu Channel* is said to apply to acts that are 'contrary to the rights'.[76] Yet, this distinction obfuscates that even if activities are prima facie lawful they may very well be 'contrary to the rights' of other states if they cause harmful effects.[77] Mere occurrence of harm can then

73 On due diligence as a general principle of international law see in the following chapter 2.C.II.

74 Coco/Dias. 'Cyber Due Diligence' 2021 (n. 64), 774.

75 Barboza, 'International Liability' 1998 (n. 14), at 330.

76 Coco/Dias. 'Cyber Due Diligence' 2021 (n. 64), 790.

77 In this vein see Alan E. Boyle, 'State Responsibility and International Liability for Injurious Consequences of Acts not Prohibited by International Law: A Necessary Distinction?', *International and Comparative Law Quarterly* 39 (1990), 1–26, at 11:

lead to state responsibility.[78] Such effects-based international wrongfulness has also been recognized in cyberspace, e.g. with regard to cyber espionage which is not per se illegal but may become unlawful if it causes harmful effects.[79] A distinction between *Trail Smelter* and *Corfu Channel* would artificially split the same legal rationale into two rules and perpetuate the flawed distinction between lawful and unlawful activities in the ILC Draft Articles on Prevention that has rightly been criticized.[80] It unnecessarily complicates an already complex terminological setting.[81]

In light of the various disadvantages of these solutions a different reference seems more promising: The harm prevention rule reflects that the rule's primary aim is the prevention of harm. It is open to integrate its due diligence component and avoids the risks of misunderstandings of the other terms. While the terminology does not directly hint at the negative prohibitive dimension regarding state-sponsored operations, one may deduce this as an argumentum *a fortiori* from the preventive dimension. The terminology 'harm prevention rule' as the 'modern' extension of the traditional no harm rule[82] has also been employed in international environmental law. As the 'harm prevention rule' lacks the disadvantages of the other

'Codifying primary environmental obligations in this way raises the question whether their breach entails a "secondary" obligation of responsibility; whether in other words the Commission's liability topic does not inevitably lead straight into State responsibility.'

78 Pointing to the *Trail Smelter* and *Corfu Channel* cases Boyle, 'State Responsibility and International Liability' 1990 (n.77), 12.

79 Such as e.g. causing a loss of functionality see Schmitt, 'Tallinn Manual 2.0' 2017 (n. 22), commentary to rule 32, p. 170, para. 6: '[I]f organs of one State, in order to extract data, hack into the cyber infrastructure located in another State in a manner that results in a loss of functionality, the cyber espionage operation violates, in the view of the Experts, the sovereignty of the latter'.

80 Boyle, 'State Responsibility and International Liability' 1990 (n.77), 22.

81 Also states understand both cases as expressions of the same rationale, see e.g. the statement by Finland which merges implicit references to both cases, Finland, International law and cyberspace, Finland's national positions, October 2020, p. 4: 'Another cardinal principle flowing from sovereignty (…) is each State's obligation not to knowingly allow its territory to be used to cause significant harm to the rights of other States'; in a similar vein Czech Republic, Comments submitted by the Czech Republic in reaction to the initial "pre-draft" report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security, March/April 2020, p. 3.

82 Brunnée, 'Procedure and Substance' 2020 (n. 67), at 148: 'In short, in international environmental law today, the "no harm rule" is the "harm prevention rule'. On the new 'harm prevention rule' see also Krieger/Peters, 'Structural Change' 2020 (n. 72), 360f.

terminological references this study hence refers to the harm prevention rule (and its due diligence aspects) as expressions of the *Island of Palmas, Trail Smelter* and *Corfu Channel* rationale.

Yet, throughout the study it important to be mindful that references to 'due diligence' are so far more prominent in cyberspace. Readers are hence cautioned that what is referred to as the harm prevention rule in this study is frequently synonymous to what other commentators and states refer to as due diligence (as an obligation or principle).

C. The doctrinal status of the harm prevention rule

So far, the study has referred to a harm prevention 'rule' without elaboration of the doctrinal basis of such an assertion.

I. The harm prevention rule as a customary rule of a general character

Due to the close link to sovereign equality the harm prevention rule belongs to a limited set of customary norms that are inherent in the structure of the international legal order. The ICJ stated with regard to such norms in *Gulf Maine*:

> '(...) customary international law (...) in fact comprises a limited set of norms for ensuring the co-existence and vital co-operation of the members of the international community, together with a set of customary rules whose presence in the opinio juris of States can be tested by induction based on the analysis of a sufficiently extensive and convincing practice, and not by deduction from preconceived ideas.'[83]

The ICJ hence distinguished between two sets of customary norms: A limited set of customary rules for the coexistence and cooperation of states and other – one may add 'ordinary' – customary rules. Similar to the ICJ the ILC distinguished 'rules framed in more general terms' from other

83 ICJ, *Case Concerning Delimitation of the Maritime Boundary in the Gulf of Maine Area (Canada/United States of America*, Judgement of 12 October 1984, ICJ Reports 1984, p. 299, para. 111.

customary rules.[84] As the harm prevention rule derives from 'generally and well recognized principles and 'elementary considerations of humanity'[85] as well as from the 'specific nature of the international community[86] the harm prevention rule – a 'fundamental rule' of international law[87] – belongs to a category of 'norms for the coexistence and cooperation' referred to by the ICJ in *Gulf Maine*. Due to their generality such rules may also be framed as customary principles[88] but to avoid doctrinal confusion this study will refer to the harm prevention rule as a customary rule of a general character. As the above dictum indicates, the generality of this customary rule is important for the required threshold of opinio iuris and state practice regarding the identification of customary international law in a specific area.[89]

II. The harm prevention rule as a general principle of international law

It has also been discussed if the harm prevention rule (or the often synonymously used 'due diligence'[90]) is a general principle of international

84 ILC, Draft conclusions on identification of customary international law, UN A/73/10, commentary to conclusion 2, p. 126, para. 5: 'The two-element approach does not in fact preclude a measure of deduction as an aid, to be employed with caution, in the application of the two-element approach, in particular when considering possible rules of customary international law that operate against the backdrop of rules framed in more general terms that themselves derive from and reflect a general practice accepted as law.'

85 ICJ, 'Corfu Channel' (n. 9), p. 22.

86 Oscar Schachter, *International Law in Theory and Practice* (Dordrecht et al.: Martinus Nijhoff 1991), 55.

87 August Reinisch/Markus Beham, 'Mitigating Risks: Inter-State Due Diligence Obligations in Case of Harmful Cyber Incidents and Malicious Cyber Activity – Obligations of the Transit State', *German Yearbook of International Law* 58 (2015), 101–112, at 106; Bäumler, 'Schädigungsverbot' 2017 (n. 55), 266: 'generelle[r] und fundamentale[r] Rechtsgedanke (…)'.

88 Report of the Secretary-General, Gaps in international environmental law and environment-related instruments: towards a global pact for the environment, UN General Assembly A/73/419, 30 November 2018, p. 7, para. 11: 'The prevention principle is well established as a rule of customary international law'.

89 See in the following chapter 2.D.

90 On inconsistent terminology see above chapter 2.B.

law.[91] It is not always clear whether references to 'general principles' or more broadly 'principles' are to be understood as doctrinal references to general principles in the sense of Art. 38 (1) lit c of the ICJ Statute, or if the reference is to be understood as referring to customary principles[92] or customary rules.[93] Both assertions of the harm prevention rule in the *Corfu Channel* and the *Trail Smelter* cases refer to it as also as a principle while it is not clear if such references to a principle are necessarily to be understood as doctrinal references.[94] ILC Special Rapporteur Marcelo Vázquez-Bermúdez highlighted the ambiguity of the term 'general principle', or 'principle', in his first report on general principles of international law:

> '(…) in practice and in the literature terms such as "principle", "general principle", "general principle of law", "general principle of international law" and "principle of international law" are often employed indistinctively and without clarification regarding which source of international law such principles belong to.'[95]

What constitutes a general principle in international law is hence notoriously contested.[96] The ILC refrained from specifying the role of general

91 Ziolkowski, 'General Principles' 2013 (n. 64), 165; referring to the general principle of due diligence Netherlands, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, Appendix, International Law in Cyberspace, p.4,5; referring to due diligence as a principle Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 13.9.2017, JOIN(2017) 450 final, 18.

92 On general principles as part of customary law Ziolkowski, 'General Principles' 2013 (n. 64), 145, 146: 'All in all, it might be wise to concur with those who claim that any intent of a rigid categorisation of general principles of international law would be inappropriate. Depending on the content and use of a principle, it can be part of customary law or a separate and substantive source in itself.'

93 The Tallinn Manual e.g. refers to due diligence both as an obligation as well as a principle, see Schmitt, 'Tallinn Manual 2.0' 2017 (n. 22), commentary to rule 6, p. 30, para. 1: '(…) the principle shall be referred to as the 'due diligence principle', as that is the term most commonly used with respect to the obligation of States to control activities on their territory'.

94 Referring to 'certain general and well-recognized principles' ICJ, 'Corfu Channel' (n. 9), p. 22; referring to the 'principles of international law'Trail Smelter' (n. 6), 1965.

95 ILC Special Rapporteur Marcelo Vázquez-Bermúdez, First report on general principles of law, A/CN.4/732, 5 April 2019, para. 254.

96 See overview Thomas Kleinlein, 'Customary International Law and General Principles Rethinking Their Relationship', in Brian D. Lepard (ed.) *Reexamining Customary International Law* (Cambridge: Cambridge University Pres 2017), 131–158. 133–

principles in the identification of customary international law in its recent study.[97] With a view to the ambiguity of the notion also highlighted by the ILC in its reports on general principles of international law[98] it does not seem helpful to affirm the harm prevention rule and its due diligence aspects as a general principle. Due to the lack of clarity over the interpretation of general principles in international law which has been lingering for decades doctrinal misunderstandings would be likely.[99] The same considerations apply to the frequently invoked, but unclear doctrinal category 'general international law'.[100]

D. Threshold of recognition in new areas of international law

To assess whether the customary harm prevention rule and its due diligence aspects have been recognized as a binding rule in cyberspace it is necessary to clarify which threshold of state practice and *opinio iuris* is required for the recognition of customary rules in cyberspace.

The methodology for identifying customary rules is an evergreen topic in discussions on the sources of international law.[101] Due to the inherent dif-

135; Stephen C. Hicks, 'International Order and Article 38(1)(c) of the Statute of the International Court of Justice' *Suffolk Transnational Law Journal* 2 (1978), 1–42, at 24f. and 27: 'general principles of law (...) [are] arguably the most important but certainly the least used and most confused source of law (...)'.

97 ILC, 'Draft conclusions on identification of customary international law, with commentaries', A/73/10, 30 April-1 June and 2 July-10 August 2018, commentary to conclusion 1, p. 124, para. 6.

98 Second report on general principles of law by Marcelo Vázquez-Bermúdez, Special Rapporteur, 9 April 2020, A/CN.4/741, p. 36, para. 114: 'Other members (…) while not outright excluding the possibility of the existence of a second category, expressed some concerns with respect to it.'

99 Rejecting categorization as a general principle Krieger/Peters, 'Structural Change' 2020 (n. 72), 376.

100 Michael Wood, 'Customary International Law and the General Principles of Law Recognized by Civilized Nations', *International Community Law Review* 21 (2019) 307–324, at 319: '[T]he term 'general international law' (…), is vague and ambiguous, and is best avoided'. See e.g. opting for analysing curstomary international law instead of the contentions notion of general international law ICJ, Separate Opinion O Donoghue' 2015 (n. 18), para. 2.

101 See James Crawford, *Brownlie's Principles of Public International Law*, 8th edition (Oxford: Oxford University Press 2012), 23–34; Andreas Paulus, 'The Judge and International Custom', *Law and Practice of International Courts and Tribunals* 12 (2013), 253–265; Brian Lepard (ed.), *Re-examining Customary International Law*

ficulty of identifying customary international law[102] a variety of approaches exists[103], but two main methodologies can be discerned: The inductive approach as the 'rulebook' approach, and what commentators have called the deductive approach[104], or deductive reasoning[105].

I. The inductive approach and its limits

The inductive approach employs the so-called 'two-elements test'. According to this two-elements test the identification of customary international law requires a general practice that is accepted as law. The ICJ has repeatedly affirmed this two-element test in its judgments[106] and also the ILC endorsed it in its recent draft conclusions on the identification of customary international law.[107] Adopting the inductive approach in cyberspace would regularly lead to the result that customary rules have not (yet) crystallized, due to states' predominant 'policy of silence and ambiguity', and

(Cambridge: Cambridge University Press 2016); Hugh W.A Thirlway, International Customary Law and Codification: An Examination of the Continuing Role of Custom in the Present Period of Codification of International Law (Leiden: Sijthoff 1972); Anthony d'Amato, *The Concept of Custom in International Law* (Ithaca: Cornell University Press 1971).

102 On the critique of the inherent uncertainty of the process of custom formation Anthea Roberts, 'Traditional and Modern Approaches to Customary International Law: A Reconciliation', *American Journal of International Law* 95 (2001) 757–791, at 767.

103 Frederic L. Kirgis, 'Custom on a Sliding Scale', *American Journal of International Law* 81 (1987), 146–151; Roberts, 'Traditional and Modern Approaches' 2001 (n. 102), 757–791.

104 ILC, 'Draft conclusions on identification' 2018 (n. 97), commentaries to csonclusion 2, p. 126, para. 5.

105 Stefan Talmon, 'Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion', *European Journal of International Law* 26 (2015), 417–443, 418.

106 ICJ, *North Sea Continental Shelf (Germany v. Denmark; Germany v. Netherlands)*, Judgment of 20 February 1969, ICJ Reports 1969, p. 3, 44; ICJ, *Jurisdictional Immunities of the State (Germany v. Italy: Greece intervening)*, Judgment of 3 February 2012, ICJ Reports 2012, p. 99, 122–123, para. 55; ICJ *Continental Shelf (Libyan Arab Jamahiriya/Malta)*, Judgment of 3 June 1985, ICJ Reports 1985, p. 13, 29–30, para. 27.

107 ILC, 'Draft conclusions on identification' 2018 (n. 97), Conclusion 2: 'To determine the existence and content of a rule of customary international law, it is necessary to ascertain whether there is a general practice that is accepted as law (opinio juris). Conclusion 3 (2): Each of the two constituent elements is to be separately ascertained. This requires an assessment of evidence for each element.'

often covert state practice.[108] Nevertheless, some states seemingly assume an inductive approach with regard to the harm prevention rule and customary rules in cyberspace in general: New Zealand for example stated that it is 'not yet convinced that a cyber-specific "due diligence" obligation has crystallized in international law'.[109] Similarly, statements of the United States (with regard to a potential sovereignty rule in cyberspace[110]), as well as Israel (with regard to the harm prevention rule and its diligence aspects[111]), suggest that they apply the inductive approach for the identification of customary rules in cyberspace. It is worth noting that the selection of states which seemingly endorse an inductive approach may not be coincidental: Demanding the high threshold of the inductive test strategically serves technologically powerful states as they will remain largely uninhibited by potentially emerging prohibitive customary rules.[112]

II. Complementary deductive considerations

Customary rules may under certain circumstances however also be derived from deduction. Deduction means that 'new rules are inferred by deductive

108 Dan Efrony/Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber-operations and Subsequent State Practice', *The American Journal of International Law* 112 (2018), 583–657, at 584; see chapter 1.D.III.

109 See New Zealand, 'The Application of International Law to State Activity in Cyberspace', 1 December 2020, para. 17.

110 Ney, 'Remarks Cyber Command' 2020 (n. 60): '(…) there is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits (…) non-consensual cyber operations in another State's territory'.

111 Roy Schondorf, Israel Ministry of Justice, Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations, 8 December 2020: '(…) we have not seen widespread State practice beyond this type of voluntary cooperation, and certainly not practice grounded in some overarching opinio juris, which would be indispensable for a customary rule of due diligence, or something similar to that, to form', available at: https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/.

112 Ann Valjataga, 'Tracing opinio juris in National Cyber Security Strategy Documents', *NATO CCDCOE 2018*, 1–18, at 5: 'Again, this rule serves a strategic purpose: not recognising obligations deriving from sovereignty allows states to conduct and respond to cyber operations against other states without breaching international law'; Michael Schmitt/Lis Vishul, 'Respect for Sovereignty in Cyberspace', *Texas Law Review* 95 (2017), 1639–1670, at 1670.

reasoning from existing rules and principles of customary international law'[113] In the *Gulf Maine* case the ICJ referred to the method as 'deduction from preconceived ideas'.[114] Commentators have highlighted that the ICJ regularly resorts to deductive interpretation in case of insufficient state practice and/or opinio iuris, inter alia to avoid a *non liquet*.[115] Also the ILC acknowledged in its recent study that deductive reasoning is an alternative way of identifying customary international law. It stated that such deviation from the inductive approach occurs 'when considering possible rules of customary international law that operate against the backdrop of rules framed in more general terms that themselves derive from and reflect a general practice accepted as law'.[116] Similarly, in his Separate Opinion in *Barcelona Traction* Judge Jessup acknowledged deviation from the inductive method with regard to '[logical rules deduced from underlying principles]'[117]. In the *Gulf Maine* the ICJ had assumed a deductive approach

113 Talmon, 'Determining Customary International Law' 2015 (n. 105), 423.

114 ICJ, 'Gulf of Maine' 1984 (n. 83), para. 111: '(...) customary international law (...) in fact comprises a limited set of norms for ensuring the co-existence and vital co-operation of the members of the international community, together with a set of customary rules whose presence in the opinio juris of States can be tested by induction based on the analysis of a sufficiently extensive and convincing practice, and not by deduction from preconceived ideas'.

115 Talmon, 'Determining Customary International Law' 2015 (n. 105), 423:The ILC in its study on the identification of customary international law also recognizes that the ICJ may occasionally need to 'develop' the law to in order to avoid a non liquet, First report on formation and evidence of customary international law by Special Rapporteur Michael Wood, 6 May-7 June and 8 July-9 August 2013, A/CN.4/66, p. 21, fn. 103: 'It is not the Court's function to develop the law, though that is occasionally what it may have to do in order to avoid pronouncing a non liquet'.

116 ILC, 'Draft conclusions on identification' 2018 (n. 97), commentary to conclusion 2, p. 126, para. 5: 'The two-element approach does not in fact preclude a measure of deduction as an aid, to be employed with caution, in the application of the two-element approach, in particular when considering possible rules of customary international law that operate against the backdrop of rules framed in more general terms that themselves derive from and reflect a general practice accepted as law'.

117 ICJ, *Barcelona Traction (Belgium v. Spain)*, Separate Opinion of Judge Jessup, Judgment of 5 February 1970, ICJ Reports 1970, 161, 197, para. 60: 'Having indicated the underlying principles and the bases of the international law regarding diplomatic protection of nationals and national interests, I need only cite some examples to show that these conclusions are not unsupported by State practice and doctrine. Where a rule of customary international law is logical, because it can be deduced from an existing underlying principle, the burden of proving the rule by way of inductive reasoning is proportionally diminished. In essence, a logical rule requires a smaller pool of state practice and opinio juris.'

with regard to '(…) a (…) set of norms for ensuring the co-existence and vital co-operation of the members of the international community'.[118]

The harm prevention rule belongs to this limited set of norms asserted by the ICJ in the *Gulf Maine* case as it arguably derives from 'elementary considerations of humanity' and the specific nature of the international community.[119] The harm prevention rule would arguably also fall under the 'logical rules' mentioned by *Judge Jessup* in his Separate Opinion in *Barcelona Traction*, due to the close link between the harm prevention rule and territorial sovereignty and sovereign equality.[120] Therefore, it is legit that the applicability of the harm prevention rule in cyberspace is approached via deductive considerations.

III. Threshold for deductive considerations

This requires a closer look at the required threshold for the deductive methodology. Some commentators have suggested that general customary rules such as the harm prevention rule do not require state consent or evidence of opinio iuris.[121] However, completely abandoning requirements of state acceptance is likely to be rejected in international practice. More convincingly, commentators have argued that taking a deductive approach does not render analysis of state practice and opinio iuris obsolete but reduces the threshold. *Worster* for example has argued that the inductive approach is not completely set aside but is complemented by deductive considerations[122], similarly to the assertion of the ILC that deduction may 'aid' the inductive approach.[123] Which precise level of state practice and opinio iuris is required under the deductive approach is not fully clear.

118 ICJ, 'Gulf of Maine' 1984 (n. 83), para. 111.
119 ICJ, 'Corfu Channel' (n. 9), p. 22.
120 See chapter 2.A.I; ICJ, 'Separate Opinion O Donoghue' 2015 (n. 18), para. 8.
121 Referring to the harm prevention rule as a general principle of international law instead of a general customary rule, yet without divergence on the substantive content of the rule Ziolkowski, 'General Principles' 2013 (n. 64), 186, 188.
122 William Thomas Worster, 'The Inductive and Deductive Methods in Customary International Law Analysis: Traditional and Modern Approaches', *Georgetown Journal of International Law* 45 (2014), 445–521, at 514: 'These deductive considerations influence the inductive process by coloring the quality of the inductive leap. (…) Thus the inductive method is not completely abandoned, but rather its application is modified by deductive conclusions.'
123 ILC, 'Draft conclusions on identification' 2018 (n. 97), commentary to conclusion 2, p. 126, para. 5.

In the *Gulf Maine* case the ICJ did not specify the required level of state practice and opinio iuris. More insightful in this regard is the Separate Opinion of Judge Jessup in the *Barcelona Traction* case in which he argued:

> 'Having indicated the underlying principles and the bases of the international law regarding diplomatic protection of nationals and national interests, I need only cite some examples to show that these conclusions are not unsupported by State practice and doctrine. Where a rule of customary international law is logical, because it can be deduced from an existing underlying principle, the burden of proving the rule by way of inductive reasoning is proportionally diminished. In essence, a logical rule requires a smaller pool of state practice and opinio juris.'[124]

The reference 'not unsupported in state practice and doctrine', as well as to 'a smaller pool of state practice and opinio iuris' shows that the threshold on the one hand is lower, but that on the other hand a certain degree of support and non-rejection by states is still required. Hence, if several states 'unsupport' or reject the application of a rule, hereby using the option to opt-out from customary rules[125], this may under some circumstances lead to so-called negative customary law.[126] States may then act as they wish to in a certain area of law. The lowering of the threshold under the deductive approach hence overall does not lead to a complete reversal of the burden of proof but a proportional diminishment.[127]

124 ICJ, 'Separate Opinion Jessup' 1970 (n. 117), para. 60, p. 197.

125 Niels Petersen, 'The Role of Consent and Uncertainty in the Formation of Customary International Law', inBrian D. Lepard (ed.) *Reexamining Customary International Law* (Cambridge: Cambridge University Pres 2017), 111–130, at 112: 'Custom, in contrast, is an opt-out system. States are bound by customary rules unless they explicitly object to their formation.'

126 Georg Dahm/Jost Delbrück/Rüdiger Wolfrum, *Völkerrecht vol 1/1 Die Grundlagen: Die Völkerrechtssubjekte* (2nd edition, Berlin: Walter de Gruyter 1989), p. 80; Silja Vöneky, 'Analogy', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia for Public International Law*, (Oxford: Oxford University Press 2008), para. 16: 'Only if so-called 'negative customary international' law exists—in a certain area of international law it is acknowledged by the relevant subjects of international law that they may act as they wish to (…)'.

127 Worster, 'Inductive and Deductive Methods' 2014 (n.122), 514: 'It would seem that where a norm is logical, because it can be deduced from another norm or social condition, the burden of proving the custom is proportionately diminished.'

IV. Endorsement of deductive considerations in cyberspace

States and commentators have endorsed this deductive approach with regard to certain customary rules in cyberspace. *Roguski* has for example argued that it is not necessary to inductively prove the applicability of every rule of international law as this applicability can already be deduced from the affirmed general applicability of the UN Charter and international law in cyberspace.[128] This view is shared by others who have argued that the 'tech-neutrality' of rules like the harm prevention rule makes the rule sufficiently broad to apply in cyberspace.[129] Also states have implicitly argued for deductive considerations. Austria has for example advocated an evolutionary interpretation of international law.[130]

As a consequence, the burden of proof for assessing the applicability of the harm prevention rule in cyberspace is proportionally diminished.[131] It still needs to be proven that the rule is not unsupported or rejected in state practice in order to conclude on the applicability of the norm.

The question *if* the harm prevention rule applies furthermore does not yet specify *how* it applies in practice. Operationability of customary norms is persistently problematic due to customary law's inherent challenges in

128 Przemysław Roguski, 'The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States', *JustSecurity*, 11 May 2020, available at: https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/.

129 Dapo Akande/Antonio Coco/Talita de Souza Dias, 'Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond', *EJIL:Talk!*, 5 January 2021, available at: https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/: 'the Corfu Channel rule of 'due diligence' (…) is sufficiently broad to be interpreted and applied to ICTs. It is the burden of those advocating for ICTs' exclusion from their scope to present evidence that states, in their general practice accepted as law, have actively carved out ICTs'.

130 Austria, Pre-Draft Report of the UN OEWG – ICT Comments by Austria, 31 March 2020, p. 2: 'For this reason, Austria does not see the "need to adapt existing international law" and is not in favour of developing "a new instrument (…) Existing law also provides an answer on how to deal legally with the problem of changing environments. Article 31(3)(b) of the Vienna Convention on the Law of Treaties foresees that when interpreting a treaty, any subsequent practice in the application of that respective treaty which establishes the agreement of the parties regarding its interpretation needs to be taken into account, together with the context.'

131 It primarily lies primarily lies on the one arguing against the applicability of a customary rule in cyberspace, Akande/Coco/Dias, 'Old Habits Die Hard' 2021 (n. 129).

'interoperationability'.[132] With regard to customary norms deduced via deductive reasoning this problem is particularly acute. Also commentators who endorse a reduced threshold for customary rules of a general character in cyberspace repeatedly assert that concretization is needed in order to make customary rules, such as the harm prevention rule, operable in practice.[133] Asserting specific measures and hereby 'micro-managing' states[134] by deduction would unduly undermine states' flexibility in implementing customary rules and in particular the harm prevention rule.[135]

V. Relevant state practice and opinio iuris in cyberspace

Relevant state practice and opinio iuris[136] regarding the endorsement of the harm prevention rule and its interpretation can be legal statements of state officials, e.g. in the UN OEWG or the UN GGE, classifications of cyber incidents[137], as well as other legal documents, e.g. documents on retorsive measures against malicious cyber operations like the EU Council Decision concerning restrictive measures against cyber-attacks.[138] Also na-

132 Jörg Kammerhofer, 'Uncertainty in the Formal Sources of International Law: Customary International Law and Some of Its Problems', *European Journal of International Law* 15 (2004), 523–553, at 551.

133 Ziolkowski, 'General Principles' 2013 (n. 64), 146, 147: '(…) it could be argued that a general principle of international law will achieve the quality of a right or obligation only after a specific interpretation of its general content in a concrete situation, making it thereby 'operational' in the legal sense.'; Moynihan, 'The Application of International Law' 2019 (n. 21), para. 75.

134 On due diligence limits regarding specificity Baade, 'The Duty to Protect' 2020 (n.70), 101.

135 On calls for specification of due diligence in cyberspace see below chapter 2.G; on specification of required measures see chapter 4.

136 State practice and opinio iuris can overlap, see ILC, 'Draft conclusions on identification' 2018 (n. 97), commentaries to conclusion 6, p. 133, para. 2: 'Given that States exercise their powers in various ways and do not confine themselves only to some types of acts (…) practice may take a wide range of forms. While some have argued that it is only what States "do" rather than what they "say" that may count as practice for purposes of identifying customary international law, it is now generally accepted that verbal conduct (whether written or oral) may also count as practice'.

137 Such as the US Cybersecurity & Infrastructure Security Agency, US-CERT Federal Incident Notification Guidelines, 1 April 2017.

138 Council of the European Union, Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 7299/19, 14 May 2019.

tional cyber security strategies can be evidence of cyber opinio iuris, or at least give insights into underlying legal reasoning of states. Even if national cybersecurity strategies do not always provide for explicit assertions of legal opinions or commitments, they can be indicators of what states are legally aspiring to or opposing.[139] Furthermore, protests against certain forms of activities or state behaviour can provide evidence of state practice.[140]

E. Recognition of the harm prevention rule in cyberspace by individual states

The harm prevention rule has received widespread endorsement by states and in the UN GGE and the UN OEWG.

I. Momentum towards recognition of the rule

Prior to 2019, recognition or even explicit mentioning of the harm prevention rule and its due diligence aspects in cyberspace was sparse. Only a CoE Report of 2011 referred to due diligence with regard to the integrity of the internet.[141] While the UN GGE Reports 2013 and 2015 entailed implicit references to the rule[142], and although commentators had pointed at the potential of harm prevention and due diligence in cyberspace for years[143]

139 Väljataga, 'Tracing opinio juris' (n. 112), 2018, p.4; asserting relevance of policy statements and strategy documents Luke Chircop, 'Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0', *Melbourne Journal of International Law* 20 (2019), 349–377, at 375.

140 ILC, 'Draft conclusions on identification' 2018 (n. 97), commentaries to conclusion 6, p. 133, para. 2: '(…) it is now generally accepted that verbal conduct (whether written or oral) may also count as practice; indeed, practice may at times consist entirely of verbal acts, for example, diplomatic protests'.

141 CoE, Steering Committee on the Media and New Communication Services (CDMC), Explanatory Memorandum to the draft Recommendation CM/Rec(2011) of the Committee of Ministers to member states on the protection and promotion of Internet's universality, integrity and openness, CM(2011)115-add1 24 August 2011, para. 78.

142 See analysis below II.2.2.

143 See Heike Krieger, 'Krieg gegen anonymous', *Archiv des Völkerrechts* 50 (2012), 1–20, at 4f.; Annegret Bendiek, 'Due Diligence in Cyberspace – Guidelines for International and European Cyber Policy and Cybersecurity Policy', *Stiftung Wissenschaft und Politik – Research Paper 2016*; Martin Ney/Andreas Zimmermann, 'Cyber-Security Beyond the Military Perspective: International Law, "Cyberspace" and the

only in 2017 a regional actor, the EU, explicitly referred to the rule as relevant in cyberspace.[144] In recent years however, significant momentum towards recognition of the rule in cyberspace can be discerned.

The harm prevention rule has been endorsed as a binding rule by a number of states, e.g. France[145], Japan[146], the Netherlands[147], Finland[148], the Czech Republic[149], Germany[150], Ireland[151] and member states of the African Union (AU).[152] The EU has persistently endorsed the rule with increasing degrees of assertiveness.[153] The harm prevention rule also enjoys strong support on the American continent. The Organization of American States (OAS) Report

Concept of Due Diligence', *German Yearbook of International Law* 58 (2015), 51–66; Bannelier-Christakis, 'Cyber Diligence' (2014) (n. 67), 23–39.

144 European Commission, Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 13 September 2017, JOIN(2017) 450 final, p. 18.

145 France, France's response to the pre-draft report from the UN OEWG Chair, OEWG 2020, p. 3.

146 Japan, Basic Position of the Government of Japan on International Law Applicable to Cyber Operations, 28 May 2021, p. 5.

147 Netherlands, 'International Law in Cyberspace' 2019 (n. 91), p. 4,5.

148 Finland, International law and cyberspace, Finland's national positions, October 2020, p.4.

149 Czech Republic, Comments submitted by the Czech Republic in reaction to the initial "pre-draft" report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security, March/April 2020, p. 3.

150 Germany, On the Application of International Law in Cyberspace Position Paper, March 2021, p.3.

151 Ireland, Position Paper on the Application of International Law in Cyberspace, July 2023, para. 2.

152 African Union, Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, 29 January 2024 (endorsed by the Assembly of the AU on 18 February 2024), para. 21.

153 Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic, 30 April 2020: 'The Council also underlined that States are not to use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts as expressed in the 2015 report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.'; Council of the European Union, 7925/17, 16 April 2018: 'The EU emphasises that States should not conduct or knowingly support ICT activities contrary to their obligations under international law, and should not knowingly allow their territory to be used for malicious activities using ICTs as it is stated in the 2015 report of the UNGGE'.

2020 noted the support of Chile, Ecuador, Guatemala, Guyana and Peru.[154] Also Iran has endorsed the structural core of the rule in its statement to the UN OEWG as a binding obligation.[155] As is typical for the harm prevention rule the terminology used in these references diverges.[156] Furthermore, states like New Zealand[157], Australia[158], Israel[159], the UK[160], South Korea[161] and

154 Chile, Ecuador, Guatemala, Guyana, and Peru all endorsed the harm prevention rule and its diligence aspects in cyberspace, see OAS, Improving Transparency': International law and State Cyber Operations (Presented by professor Duncan B. Hollis), 5th Report, CJI/doc. 615/20 rev.1, 7 August 2020, para. 48.

155 Iran, Zero draft report of the Open-ended working group On developments in the field of information and telecommunications in the context of international security, UN OEWG, January 2021, p. 13: 'States should ensure appropriate measures with a view to making private sector with extraterritorial impacts, including platforms, accountable for their behaviour in the ITC environment. States must exercise due control over ICT companies and platforms under their (…) jurisdiction, otherwise they are responsible for knowingly violating national sovereignty, security and public order of other states.'

156 States refer both to the 'duty to prevent significant harm', 'due diligence' or infer the duty 'not to knowingly allow their territory to be used contrary to the rights of other states' or use further divergent formulations. On divergent terminology regarding the harm prevention rule and due diligence, reflecting the historical evolution of the rule, see chapter 2.B.

157 New Zealand, 'International Law in Cyberspace' 2020 (n.109), para. 17.

158 Australia's International Cyber Engagement Strategy, October 2017, p. 91: 'To the extent that a state enjoys (…) sovereignty over objects and activities within its territory, it necessarily shoulders corresponding responsibilities to ensure [they] are not used to harm other states (…)'.

159 Schondorf, 'Israel's Perspective' 2020 (n.111): '(…) The inherent different features of cyberspace – its decentralization and private characteristics – incentivize cooperation between States on a voluntary basis, such as with the case of national Computer Emergency Response Teams (CERTs). CERTs are already doing what could arguably fall into that category: exchanging information with one another, as well as cooperating with each other in mitigating incidents. However, we have not seen widespread State practice beyond this type of voluntary cooperation, and certainly not practice grounded in some overarching opinio juris, which would be indispensable for a customary rule of due diligence, or something similar to that, to form'.

160 UK Comments on Zero Draft Report of the UN OEWG On Development in the Field of ICTs in the Context of International Security, 2021, p. 3: 'This paragraph should end at this point given differences of opinion as to the existence of a legally binding obligation of 'due diligence' in cyberspace.'

161 Republic of Korea, Comments on the pre-draft of the UN OEWG Report, 14 April 2020, p. 5: 'The ROK believes that the international community should embark on discussions to review the legal status of due diligence to be elevated as a legal obligation. However, the ROK also recognizes that States' views on this matter may vary and it will take more time to come to an agreement.'

Canada[162] have expressed support or acknowledge the relevance of the rule in cyberspace even if they do not view it as a binding rule (yet). The US has so far remained silent on the issue in the OAS Report but mentioned the concept's relevance in cyberspace before.[163] Argentina argued that the harm prevention rule is not a binding rule in cyberspace. It however did not elaborate whether it rejects the rule in general.[164] Uncertainty as to the rule's content may have provoked the caution of states to commit to the rule.[165] Hence, even the more cautious assertions of opinio iuris support the argument that the applicability of the rule in cyberspace is largely approved. Importantly, no state has developed a substantial critique of the rule's relevance in cyberspace. Furthermore, it is notable that a significant number of states from differnet cyber security 'camps' have endorsed the rule, from Western states, to so-called 'digital swing states[166]' on the American continent, to states like Iran which frequently takes opposing positions in the international legal discourse on cyber security matters.[167]

---

162 Canada, UN OEWG 2020, 4: Canada considers that States have a responsibility to ensure that their territory is not used in a way that harms the rights of other States; The reference to 'responsibility', as opposed to duty or obligation suggests that Canada is adopting the assumption that no harm / due diligence is non-binding, as stated in para. 13c UN GGE Reports 2015.

163 Referring to cyber security due diligence primarily in a self-protective sense US, International Strategy for Cyberspace, May 2011, p. 10.

164 See statement by Argentina in the Open-ended working group on developments in the field of information and telecommunications in the context of international security – Second substantive session, 10–14 February 2020, available at: https://media.un.org/en/asset/k18/k18w6jq6eg at minute 02:15:05.

165 Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views', *The Hague Program for Cyber Norms, Policy Brief,* March 2020, p. 11; Moynihan, 'The Application of International Law' 2019 (n. 21), para. 75.

166 On digital swing states see Tim Maurer/Robert Morgus, *Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate* (The Centre for International Governance Innovation and the Royal Institute for International Affairs 2014).

167 The split between different 'camps' is exemplified by the parallel adoption of two competing resolutions in the UN General Assembly in 2018: One (UN General Assembly Resolution A/RES/73/27) was sponsored by Russia and like-minded states and created the UN OEWG. The other (UN General Assembly Resolution A/RES /73/266) was sponsored by the US and like-minded states and extended the mandate of the UN GGE. Due to the support of several swing states the UN General Assembly approved both but both 'camps' rejected the resolution introduced by the other camp, see *Alex Grigsby, 'The* United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased', *Council on Foreign Relations,* 15 November

II. Concern and pushback

Some states have nevertheless raised several concerns against the application of the rule in cyberspace. While these concerns have not led to a rejection of the rule in cyberspace they need to be highlighted for a comprehensive picture of states' opinio iuris on the rule.

1. Concern about over-securitization

Several states and commentators have voiced the concern that the preventive aspect of due diligence may lead to an over-securitization of cyberspace with detrimental impacts on human rights, e.g. through extensive monitoring of cyber activities.[168] While concerns about over-securitization are well-reasoned regarding the push of authoritarian states to exercise tighter control over cyberspace[169] this concern can be mitigated by a sound legal interpretation of the requirements of reasonable diligence measures.[170] As asserted by the ICJ in *Bosnia Genocide*, due diligence requirements have to be interpreted in compliance with other rules of international law, in particular with human rights law.[171] A human rights-compliant interpretation of diligence requirements is for example particularly relevant with regard to criminal procedural law.[172] Also states' measures to acquire

2018, available at: https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

168 New Zealand bases its rejection of the bindingness of the rule on the argument that '[i]t is clear that states are not obliged to monitor all cyber activities on their territories or to prevent all malicious use of cyber infrastructure within their borders', New Zealand, 'International Law in Cyberspace' 2020 (n.109), para. 17; see also Schmitt, 'Tallinn Manual 2.0' 2017 (n. 22), commentary to rule 7, p. 45, para. 8: 'The Experts further noted that the obligations of States under international human rights law could run counter to such a [preventive] duty, depending on how it was fulfilled'.

169 See on risks e.g. for freedom of expression Krieger/Peters, 'Structural Change' 2020 (n. 72), 386.

170 Liisi Adamson, 'Recommendation 13c', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 49–75, p. 72, para. 34.

171 ICJ, 'Bosnia Genocide' 2007 (n. 40), para. 430.

172 On human rights safeguards against overly expansive investigatory competences in domestic criminal procedural law see chapter 4.D.I.5.2.

knowledge about cyber activities on their territories, e.g. via monitoring measures, need to comply with human rights law.[173] The concern about a due diligence-incentivized over-securitization of cyberspace is hence not insurmountable and should not be overemphasized.

2. Capacity concerns

Some states and commentators are concerned that a binding due diligence obligation may overburden states with limited technological capacity. Bolivia has highlighted that a state should not be held liable under due diligence when it lacks the technological capacity to control a non-state actor.[174] The Tallinn Manual was concerned that a duty to prevent would overburden states as the 'difficulty of mounting comprehensive (…) defences against all cyber threats (…) would impose an undue burden on states'.[175]

However, also the concerns about an undue burden can be mitigated via a sound interpretation of due diligence requirements. As was noted above, the required standard of diligent harm prevention (reasonable care) takes the subjective capacity of a state and the overall feasibility of a measure into account.[176] States and commentators have underlined this capacity-dependent variability of the rule in cyberspace.[177] Only with regard to an ob-

173 In more detail see chapter 4.B.3.

174 On the equivocality of the assertion OAS, 'Improving Transparency – 5th Report' 2020 (n. 239), p. 32, paras. 49, 50: '(…) This view could be consistent with having due diligence as an international legal rule for cyber operations as due diligence generally has required States to "know" about the activities in question, which may not be possible for States lacking the requisite technical infrastructure (…) On the other hand, the inability to "control" cyber activities of which it has knowledge might suggest Bolivia does not accede to the due diligence doctrine in cyberspace. Without further clarification of Bolivia's response, it is difficult to reach a conclusion one way or another.'

175 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 22), commentary to rule 7, p. 45, para. 8.

176 See above chapter 2.E.II.2; ILA, Second Report 2016 (n. 19), 2016, p. 3; ILC, 'Draft Articles on Prevention' 2001 (n.37), commentaries to art. 3, p. 55, para. 17.

177 Czech Republic stressed the interlinkage between capacity and due diligence in the UN OEWG, 'Comments' (n. 149) 2020, p. 3; see also AU, 'Common African Position' 2024 (n.152), para. 22; CoE, 'Memorandum' (n.141), 2011, para. 81; Reinisch/ Beham, 'Mitigating Risks' 2015 (n.87) 2; Coco/Dias, 'Cyber Due Diligence Report' 2021 (n. 48), 165; Monnheimer, 'Due Diligence Obligations' 2021 (n. 1), 197ff.: 'Therefore, limited capacities play a most significant role also with regard to cyber diligence obligations, with many authors supporting varying standards of care.'

jective international minimum standard the capacity-dependent variability of the diligence may be limited but it is acknowledged that some minimum requirements, such as legislative or administrative measures, are measures that every government can be expected to take, regardless of capacity.[178] The concern of the Tallinn Manual about the impossibility of comprehensive defences 'against all cyber threats' overlooks the character of the harm prevention rule as an obligation of conduct. The duty to prevent does not require that all cyber threats are in fact prevented. It suffices that states exercise due diligence to prevent harm; if harm occurs despite diligent state behaviour the state will not be held liable.[179] The concern about over-burdening states hence eventually does not hold water.

F. Recognition of the rule on the UN level

Evidence of the recognition of the harm prevention rule can also be found on the UN level, hereby corroborating that states support the harm prevention rule's applicability in cyberspace.

I. Endorsement of the harm prevention rule in the UN GGE Reports

On the global level, the most important legal documents are the Reports of the UN GGE of 2013, 2015 and 2021. The Reports were furthermore welcomed by the UN General Assembly[180] which is relevant as resolutions of the UN General Assembly, despite their non-binding character – may provide evidence for determining the existence of a rule of customary international law.[181] With regard to the harm prevention rule the UN GGE Report 2013 asserted:

178 ILC, 'Draft Articles on Prevention' 2001 (n.37), commentaries to art. 3, p. 155, para. 17.

179 ICJ, 'Bosnia Genocide' 2007 (n. 40), para. 430; see also chapter 5.A.I. on consequences of negligence.

180 UN General Assembly Resolution A/RES 68/243, 9 January 2014, preambular para.11; UN General Assembly Resolution A/RES/70/237, 30 December 2015, paras. 1,2.

181 ILC, 'Draft conclusions on identification' 2018 (n.97), conclusion 12.

> 'States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs'[182]

This formulation was reasserted, with minor modifications, in Part VI of the UN GGE Report 2015 on international law:

> '(…) States (…) should seek to ensure that their territory is not used by non-State actors to commit such [i.e. internationally wrongful] acts'[183]

In the part on norms, rules and principles for the responsible behaviour of states the UN GGE Reports 2015 furthermore stipulated that:

> 'States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.'[184]

Beyond these two references one may assume a third implicit reference to the harm prevention rule in the reference to '*norms and principles that flow from sovereignty*' which are said to apply in cyberspace.[185]

None of these formulations directly refer to the harm prevention rule or due diligence but they are clearly reminiscent of the ICJ dictum in *Corfu Channel* regarding a state's duty 'not to allow knowingly its territory to be used contrary to the rights of other states'. It is therefore consequent that both states and commentators interpret in particular para. 13 lit. c as references to the harm prevention rule.[186] The consensus expressed by the UN GGE Reports is significant as states from various 'blocks', including states from the Shanghai Cooperation Organization (SCO), such as Russia and China, Western states, as well as digital 'swing' states[187], such as

182 United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013 (UN GGE Report 2013), para. 23.

183 UN GGE Report 2015; Part VI (international law), paras. 24–29, para. 28e.

184 UN GGE, Report 2015, Part III (Norms, rules and principles for the responsible behaviour of States), paras. 9–15, para. 13c; reiterated and supplemented with additional guidance in UN GGE Report 2021, paras. 29, 30.

185 UN GGE, Report 2015, para. 27. As laid out above, the harm prevention rule derives from territorial sovereignty and sovereign equality and hereby arguably 'flows from sovereignty', see chapter 2.A.I.

186 Republic of Korea, 'Comments' 2020 (n.161), p. 5; Schondorf, 'Israel's Perspective' 2020 (n.111); Adamson, 'Recommendation 13c' 2017 (n.170) p. 49, para.2; Eric Talbot Jensen, 'Due Diligence in Cyber Activities', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 252–269, at 253.

187 On digital swing states see Maurer/Morgus, 'Global Swing States' 2014 (n.166).

Brazil, supported the reports.[188] The UN GGE Reports are furthermore important reference documents for the international legal discourse and are referenced by regional and state actors[189], e.g. in the UN OEWG or in MoU.[190] This further corroborates the conclusion that the applicability of the harm prevention rule is recognized in cyberspace.

II. Problematic terminology of the UN GGE Reports

Nevertheless, one may raise several caveats against the endorsement of the harm prevention rule in the UN GGE Reports. A first caveat is due to the terminology with which the harm prevention rule is referenced in the UN GGE Report 2015. Para. 13 lit. c refers to *internationally wrongful acts*.[191] This formulation is misleading: *Internationally wrongful acts* in the sense of Art. 2 of the ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA) require a violation of an international legal obligation that is attributable to a state.[192] If, following a strict textual

188 Pointing at the broad participation in the UN GGE process also Kubo Mačák, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers ', *Leiden Journal of International Law* 30 (2017), 877–899, at 881.

189 The UN GGE norms were e.g. mentioned in a joint proposal in the UN OEWG which was supported by a number of states from all continents, see Open Ended Working Group Developments in the field of information and telecommunications in the context of international security, Joint Proposal of Argentina, Australia, Canada, Chile, Denmark, Estonia, France, Indonesia, Kenya, Mexico, the Netherlands, New Zealand, Pacific Island Forum member states, Poland, and South Africa, 16 April 2020: '[Member states are call[ed]' upon (…) to be guided in their use of information and communications technologies by the 2015 report of the Group of Governmental Experts and that A/70/74 recommended Member States "give active consideration to the reports and assess how they might take up these recommendations for further development and implementation".

190 ASEAN-EU Statement on Cybersecurity Cooperation, 1 August 2019, para. 6: 'We recall that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability (…) We also recall the conclusions of the 2010, 2013 and 2015 Reports of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, as endorsed by the UN General Assembly'.

191 UN GGE Report 2015, para. 13 lit.c: 'States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs'.

192 ILC, Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), UN General Assembly, A/56/10, 23 April-1 June, 2 July-10 August 2001, Article 2: 'Elements of an internationally wrongful act of a State – There is an internationally wrongful act of a State when conduct consisting of an action or

reading of para. 13 lit. c, an internationally wrongful act was required this would exclude acts of non-state actors which are not attributable to a state as acts of non-state actors in principle do not constitute internationally wrongful acts. It is however precisely one of the primary benefits of the harm prevention rule to provide an accountability mechanism for acts of non-state actors which are *not* attributable to states.[193]

Nevertheless, some commentators consider it possible that indeed the UN GGE may have wanted to restrict the scope of para. 13 lit. c.[194] Given that such a restriction would drastically undermine the rule's applicability this seems unlikely.[195] Furthermore, it would run counter to the parallel formulation in para 28 lit. e of the UN GGE Reports and the UN OEWG Predraft which are formulated more openly and refer to 'such acts' (equivalent to an internationally wrongful act mentioned earlier in the norm) committed by non-state actors.[196] Also the additional guidance in the UN GGE Report 2021 – despite adopting the reference to internationally wrongful acts – simultaneously suggests that acts of non-state actors come under

omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State.' Art. 2 thus stipulates attribution as a constituent element of the international wrongfulness of an act. In another part the commentaries however separate the question of the international wrongfulness from the question of attribution: '(…) Attribution must be clearly distinguished from the characterization of conduct as internationally wrongful (sic) Its concern is to establish that there is an act of the State for the purposes of responsibility. To show that conduct is attributable to the State says nothing, as such, about the legality or otherwise of that conduct, and rules of attribution should not be formulated in terms which imply otherwise (…) In this respect there is often a close link between the basis of attribution and the particular obligation said to have been breached, even though the two elements are analytically distinct', see also ibid., commentaries to art. 3, p. 39, para. 5.

193 Peters/Krieger/Kreuzer, 'Dissecting the Leitmotif' 2020 (n. 38) 4; Antal Berkes, 'The Standard of 'Due Diligence' as a Result of Interchange between the Law of Armed Conflict and General International Law', *Journal of Conflict & Security Law* 23 (2018), 433–460, at 440.

194 Adamson, 'Recommendation 13c' 2017 (n.170), p. 58, para. 17.

195 Also statements of states in the UN OEWG weigh against a restrictive reading of para. 13c: Austria e.g. separates the question of the attribution of an act to a state from the question whether it was internationally wrongful see Austria, 'Comments' 2020 (n.130), p. 3.

196 UN OEWG, Revised pre-draft, para. 30: 'States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts.'; UN GGE Report 2015, para. 28e: '(…) States (…) should seek to ensure that their territory is not used by non-State actors to commit such [i.e. internationally wrongful] acts'.

the purview of the rule.[197] Furthermore, several states and commentators have resorted to more open formulations that avoid the doctrinal intricacies of the reference to internationally wrongful acts, such as 'serious adverse consequences'[198], significant harm[199], or significant harmful effects.[200] Ecuador[201] combined reference to 'internationally wrongful acts' with the more open-ended reference to 'serious adverse consequences'. Therefore, an area-specific restriction of the harm prevention rule intended by the formulation in para. 13 lit. c of the UN GGE Report 2015 seems unlikely. The undesirable consequences of a strict textual reading of para. 13 lit. c may be overcome by reading an unwritten addition – 'if committed by the state' – into it.[202]

197 UN GGE Report 2021, para. 29: '(…) if a State is aware of or is notified in good faith that an internationally wrongful act conducted using ICTs is emanating from or transiting through its territory it will take all appropriate (…) steps (…) It conveys an understanding that a State should not permit another State or non-State actor to use ICTs within its territory to commit internationally wrongful acts.'

198 Ecuador preliminary comments to the Chair's "Initial pre-draft" of the Report of the United Nations Open Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG), p.2; Schmitt, 'Tallinn Manual 2.0' 2017 (n. 22), commentary to rule 6, para. 21: 'The International Group of Experts identified no convincing rationale for excluding non-State actor cyber operations having serious adverse extraterritorial consequences from the ambit of the State's due diligence obligation (…)'.

199 Finland, 'International law and cyberspace' 2020 (n. 148), p. 4; CoE, 'Memorandum' (n.141), 2011, para. 81.

200 New Zealand, 'International Law in Cyberspace' 2020 (n.109), para. 14: 'Bearing those factors in mind, and having regard to developing state practice, New Zealand considers that territorial sovereignty prohibits states from using cyber means to cause significant harmful effects manifesting on the territory of another state'.

201 Ecuador preliminary comments to the Chair's "Initial pre-draft" of the Report of the United Nations Open Ended Working Group on developments in the field of information and telecommunications in the context of international security (UN OEWG). April 2020, p.2.

202 See with a similar formulation in the context of complicity Schmitt, 'Tallinn Manual 2.0' 2017 (n. 22), rule 18: 'With respect to cyber operations, a State is responsible for: (a) its aid or assistance to another State in the commission of an internationally wrongful act when (…) the act would be internationally wrongful if committed by it; (b) the internationally wrongful act of another State it directs and controls if the direction and control is done with knowledge of the circumstances of the internationally wrongful act and the act would be internationally wrongful if committed by it (…).'

1. Hortatory language of the UN GGE Reports

A further caveat regarding the recognition of the harm prevention rule in the UN GGE Reports concerns its bindingness. The UN GGE reports employ deliberately hortatory language. The harm prevention rule reference in para. 13 lit. c of the UN GGE Report 2015 is part of what the UN GGE Report coins 'non-binding, voluntary norms of responsible state behavior'.[203] The implicit reference in para. 28 lit. e UN GGE Report 2015 moreover employs the weaker formulation 'should seek to ensure' instead of 'shall'.[204] The report also structurally distinguishes between norms of responsible state behaviour, such as the harm prevention rule (Part III), and international law (Part VI) which suggests that the harm prevention rule is relegated to the level of a mere voluntary norm in cyberspace.[205]

The statements of several states however weigh against drawing such a conclusion. China has stressed in the UN OEWG that the emphasis on the voluntary nature of the UN GGE norms may send the 'unconstructive message to the world that we are unwilling to abide by the hard-won norms established through strenuous negotiations'.[206] Also Russia has dismissed attempts to weaken the legal status of the norms of the UN GGE Reports 2015.[207]

States have moreover increasingly recognized the potential friction between asserting allegedly non-binding rules and asserting the applicability of binding rules of international law. Numerous states have asserted that the norms of para. 13 of the UN GGE Report 2015 are 'complementary' to inter-

203 UN GGE, Report 2015, Part III (Norms, rules and principles for the responsible behaviour of States), paras. 9–15.

204 UN GGE Report 2015, para. 28 lit. e.

205 This distinction was also taken up by the UN OEWG Reports see UN OEWG, Final Report 2020, para. 34–40; Zero Draft Part D; on 'Rules, Norms and Principles for Responsible State Behaviour' see UN OEWG, Final Report 2020, para. 24–33; Zero Draft, Part C; and the UN GGE UN GGE Report 2021, on 'Norms, Rules and Principles' paras. 15–68; on international law paras. 69–73.

206 China's Contribution to the Initial Pre-Draft of OEWG Report, 2020, p. 2,3.

207 Russian Federation, Commentary of the Russian Federation on the Initial 'Re-Draft' of the Final Report of the United Nations Open-Ended-Working-Group, p. 3: '(…) the text insistently promotes 11 norms of the 2015 GGE report that were directly and fully reflected in the abovementioned resolution, which gives them a completely different status than just a call to the States to be guided by them.'

national law.[208] Close to complementarity the UN GGE Report 2021 asserted that norms and rules 'sit alongside each other'.[209] Complementarity, as opposed to alternative, suggests that the inclusion of a norm in Part III on norms in the UN GGE Report 2015 should not undermine the legal status of applicable legal rules.[210] In a similar vein, the UN OEWG Final Report affirmed that the characterization as a norm of responsible state behavior does not weaken the binding character of existing legal obligations:

> '(…) [N]orms do not replace or alter States' obligations or rights under international law, which are binding, but rather provide additional specific guidance on what constitutes responsible State behaviour in the use of ICTs (…)'[211]

Lastly, the UN OEWG Zero Draft referred to the '*reinforcing* and complementary' character of the norms[212], and the UN GGE Report 2021 noted that norms 'reflect the expectations of the international community and set standards for responsible state behaviour'.[213] This further supports the argument that the inclusion of a norm as a norm of responsible state behaviour in para. 13 of the UN GGE Report should not weaken its legal status. Therefore, the characterization as a non-binding norm should not be overemphasized.[214] States are however well advised to reconsider this

208 UN OEWG, 'Pre-draft Report', 2020, para. 26; Germany, Non-paper listing specific language proposals under agenda item "Rules, norms and principles" from written submissions received before 2 March 2020, Comments from Germany, 2 April 2020, p. 2: 'existing international law, complemented by the voluntary, non-binding norms that reflect consensus among States, is currently sufficient for addressing State use of ICTs'; Germany has also referred to the 'supplementary' character of norms of responsible state behaviour Germany, 'Application of International Law' 2021 (n.150).

209 UN GGE Report 2021, para. 15.

210 Akande/Coco/Dias, 'Old Habits Die Hard' 2021 (n. 129).

211 UN OEWG Final Report, para. 25.

212 UN OEWG Zero Draft Report 2021, para. 117. The formulation was omitted in the Final Report.

213 UN GGE Report 2021, para. 15.

214 Akande/Coco/Dias, 'Old Habits Die Hard' 2021 (n. 129): 'Thus, the mere fact that states have decided, for whatever political reason, to mirror existing rules of international law in their policy recommendations cannot free the former of their binding legal force (…) Thus, compliance with several norms of responsible state behaviour in cyberspace is not only expected on a voluntary basis, but also required as a matter of applicable international law.'; in more detail see also Coco/Dias, 'Cyber Due Diligence Report' 2021 (n. 48), 61; in a similar vein, Canada emphasized that the characterization of a norm as voluntary and non-binding does not preclude

'bucketing of norms'[215] between 'norms and rules' as a certain ambiguity regarding the relationship of norms and rules may weaken the status of applicable legal rules in the long-term.[216]

2. Permissive assertions of freedom of action

A further indirect challenge to the bindingness of the harm prevention rule in cyberspace may be an assertion that is present both in the UN GGE Reports, as well as in the UN OEWG Final Report:

> 'Norms [of responsible state behaviour][addition by the author] do not seek to limit or prohibit action that is otherwise consistent with international law.'[217]

Such permissive assertions, if embraced more broadly by states, would present a significant challenge to the applicability of prohibitive international legal rules in their cyber-specific interpretation, including the harm prevention rule. The assertions are not directed at the harm prevention rule or other preventive rules. However, the question which activities international law *limits* or which threshold of harm is prohibited in cyberspace is precisely the core question which the UN OEWG and the UN GGE need to address with regard to cyber harm below the threshold of a prohibited intervention ('low-level' cyber harm). A permissive stance along the lines of para. 15 of the UN GGE Report of 2021, somewhat reminiscent of the rationale of the Permanent Court of International Justice (PCIJ) in *Lotus*[218]

---

its recognition as a binding legal rule', Canada, International Law Applicable in Cyberspace, April 2022, para. 26, fn. 20;; also critical of the alleged shift from hard to soft law norms Samantha Besson, 'La Due Diligence en Droit International', *Recueil des Cours de l'Académie de Droit International de la Haye* 409 (2020) 153–398, at 341, para. 452.

215 Eneken Tikk, 'Introduction', in Enekken Tikk (ed.), Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary (United Nations Office for Disarmament Affairs 2017), p. 4.

216 On states' strategic avoidance of accountability mechanisms in cyberspace and consequent problems for the operationalization and development of international law see already above chapter I.D.III.

217 UN OEWG, Final Report 2020, para. 25.; UN GGE Report 2021, para. 15; UN GGE Report 2015, para. 10.

218 PCIJ, *The Case of the S.S. Lotus (France v. Turkey)*, Judgment of 7 September 1927, Series A, No. 10, at 18: 'Far from laying down a general prohibition (…) States may

and the permissive notion of 'external sovereignty' in the Tallinn Manual[219] does not do justice to the current discussions around an international legal norm against low-level cyber harm. It may be particularly favoured by states which also assert an inductive approach to the determination of international legal rules[220] due to a likely preference for uninhibited state action in cyberspace. Such an approach however risks creating a serious element of instability in international relations and effectively undermines the attempts of the very same states to contribute to norm development and stability in cyberspace in the UN GGE or the UN OEWG. It remains to be seen whether states embrace such assertions in the near future.

G. Need for specification in cyberspace

Overall, the above-mentioned documents show that the harm prevention rule has also found broad recognition on the UN level. While the specific assertions in the UN GGE are deliberately hortatory and exemplify states' preference for strategic ambiguity, weaknesses in the current formulations should not be overemphasized. So far, they provide no indication that states 'unsupport' or reject the rule. The UN GGE Reports hence largely concur with the cautious, but steadfast endorsement of the rule by individual states. It therefore can be assumed that the required threshold for the recognition of the rule in cyberspace is met and that the harm prevention rule (including its due diligence requirements) applies as a binding rule in cyberspace.

The assertion that the rule applies does not yet answer *how* it applies. In discussions in the UN OEWG states have repeatedly called upon other states to specify their understanding of the harm prevention rule in cyber-

not extend the application of their laws and the jurisdiction (…) [international law] leaves them in this respect a wide measure of discretion, which is only limited in certain cases by prohibitive rules'.

219 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 22), rule 3: 'A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it'.

220 See the above-mentioned position of New Zealand, 'International Law in Cyberspace' 2020 (n. 109), para. 17; UK AG Wright, 'Cyber and International Law' 2018 (n. 60).

space[221], e.g. the Netherlands[222] or South Korea.[223] The question is not so much *if* a general customary rules applies in cyberspace but rather *how* it is applied. This was e.g. emphasized by Austria in its statement in the UN OEWG:

> '[W]e believe that when talking about "gaps", we are not referring to the set of legally binding rules of international law as such, but rather to the interpretation of these rules in the cyber context and to the issue of how to apply these obligations against this background.'[224]

Akande/Coco/Dias have referred to this need for specification through acknowledging the need to 'tie loose ends'.[225] Taking a constructivist perspective, one may argue that it is necessary to 'tie loose ends' to move from gradual norm acceptance towards norm internalization.[226] A repository, as envisioned in the UN OEWG, e.g. by the NAM states[227], or an official

221 UN OEWG, 'Zero Draft Report 2021, paras. 32, 48; UN OEWG, 'Pre-draft Report 2020, para. 37: 'While these norms articulate what actions States should or should not take, States underscored the need for guidance on how to operationalize them'.

222 Netherlands, The Kingdom of the Netherlands' response to the pre-draft report of the UN OEWG, 2020, p. 4.

223 Republic of Korea, 'Comments' 2020 (n. 161), p. 5: 'In order to effectively respond to increased cyber threats in the meantime, it is necessary to concretize and clarify what is already agreed.'

224 Austria, 'Comments' 2020 (n.130), p. 2.

225 Akande/Coco/Dias, 'Old Habits Die Hard' 2021 (n. 129): '[W]hen applying general rules of existing international law to new technologies, some loose ends may need to be tied and adjusted with best implementation practices to account for certain specific features'; on the need for specification Liisi Adamson, 'Recommendation 13c', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 49–75, at 75, para. 40.

226 See Martha Finnemore/Kathryn Sikkink, 'International Norm Dynamics and Political Change', *International Organization* 52 (1998), 887–917, at 895; the authors describe a three-stage process (from norm emergence to norm acceptance to norm internalization). Due to the broad endorsement of the harm prevention rule and no principled objection against it one may argue that the tipping point for the stage of norm acceptance has been reached.

227 Non-Aligned Movement, NAM Working Paper for the Second Substantive Session of the Open-ended Working Group on developments in the Field of Information and Telecommunications in the Context of International Security (UN OEWG), January 2021, p. 1: 'Member States should be encouraged to compile and streamline the information that they presented on their implementation of international rules and the relevant proposed repository (…)'.

compendium suggested by the UN GGE Report 2021[228], could help in this regard. Regarding the question how the harm prevention rule applies in cyberspace especially two questions need to be concretized: On the one hand which threshold of cyber harm triggers due diligence duties to prevent[229] and on the other hand which specific measures due diligence requires.[230]

228 UN GGE Report 2021, para. 73: '(…) an official compendium [document symbol to be provided] of voluntary national contributions of participating governmental experts on the subject of how international law applies to the use of ICTs by States will be made available (…) The Group encourages all States to continue sharing their national views and assessments voluntarily through the United Nations SecretaryGeneral and other avenues as appropriate'.

229 See in the following chapter 3.

230 See in the following chapter 4.

Chapter 3: The Threshold for Triggering Due Diligence Obligations to Prevent

A. General Criteria

It is challenging to determine when due diligence obligations for harm prevention are triggered.[1] If any risk of harm triggered preventive duties this would likely be overly intrusive upon state sovereignty as it is inevitable that in an increasingly interconnected international legal order states will influence each other and at times also in a detrimental way.[2] It is hence clear that minor harmful effects and mere nuisances have to be tolerated and do not trigger due diligence obligations to prevent. In principle, any 'wrong' or 'injurious act' that affects the rights of other states can fall under the purview of the harm prevention rule.[3] Interference with a right of a state will regularly indicate that the threshold is met.[4] These abstract enunciations as such do however not say anything meaningful about the precise threshold of when due diligence duties are triggered.

I. Risk of significant cyber harm

In the *Trail Smelter* arbitration the tribunal referred to 'serious consequences'.[5] In its Draft Articles on Prevention the ILC asserted the threshold of 'risk of significant harm', distinguishing it from the allegedly higher

1 Luke Chircop, 'A Due Diligence Standard of Attribution in Cyberspace', *International and Comparative Law Quarterly* 67 (2018), 1–26, at 8; Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press 2017), p. 36, para. 25.

2 Jelena Bäumler, *Das Schädigungsverbot im Völkerrecht* (Berlin: Springer 2017), 5.

3 US Supreme Court, *United States v. Arjona*, 7 March 1887, 120 U.S. Reports 1887, 484; *Trail Smelter Case (USA v. Canada)*, Decision of 16 April 1938, UNRIAA, vol. III, 1963; ICJ, *Corfu Channel Case (United Kingdom v. Albania),* Judgment of 9 April 1949, ICJ Reports 1949, 4, p. 22. see chapter 2.A.II.

4 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), p. 34, para. 15.

5 Trail Smelter' (n. 3), 1965.

standard of 'seriousness', 'substantial' or 'grave' harm.[6] The ICJ reiterated the threshold of a risk of significant harm in *Pulp Mills*.[7] As the threshold of significant harm is also stipulated in several treaty norms which spell out the harm prevention rule area-specifically[8], it can be considered the most dominant threshold for triggering due diligence duties.

In cyberspace, this 'significance' threshold has been acknowledged by a variety of states and commentators.[9] Finland for example reiterated the 'significant harm' threshold.[10] The (non-binding) Paris Call for Trust and Security condemned 'significant, indiscriminate harm'[11], a CoE Report asserted the significance threshold regarding harm to the integrity and availability of the internet.[12] Other states have used broader formulations. The Czech Republic e.g. referred to harm to states' rights.[13] France broadly

6 ILC, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, UN General Assembly, A/56/10, 23 April-1 June, 2 July-10 August 2001, commentary to art. 2, 152, para. 4.

7 In the judgment the ICJ referred to 'significant damage' ICJ, Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment of 20 April 2010, ICJ Reports 2010, p.14, 45, para. 101.

8 OECD Council recommendation C(74)224 of 14 November 1974 on Principles concerning transfrontier pollution (OECD, OECD and the Environment (1986), p. 142); Helsinki Rules on the Uses of the Waters of International Rivers (International Law Association, Report of the Fifty-second Conference, Helsinki, 1966 (1967), p. 496), article X; Memorandum of Intent Concerning Transboundary Air Pollution, between the Government of the United States and the Government of Canada, of 5 August 1980 UNTS vol. 1274, No. 21009, p. 235.

9 Rebecca Crootof, 'International Cybertorts: Expanding State Accountability in Cyberspace', *Cornell Law Review* 103 (2018), 565–644, at 600.

10 Finland, International law and cyberspace, Finland's national positions, October 2020, p.4: 'It is widely recognized that this principle, often referred to as due diligence, is applicable to any activity which involves the risk of causing significant transboundary harm.'; similarly, New Zealand has referred to significant harmful effects, albeit only with regard to the negative prohibitive dimension, New Zealand, The Application of International Law to State Activity in Cyberspace, 1 December 2020, para. 14: 'Bearing those factors in mind, and having regard to developing state practice, New Zealand considers that territorial sovereignty prohibits states from using cyber means to cause significant harmful effects manifesting on the territory of another state'.

11 Paris Call for Trust and Security, 12 November 2018, p. 1.

12 Explanatory Memorandum to the draft Recommendation CM/Rec(2011) of the Committee of Ministers to member states on the protection and promotion of Internet's universality, integrity and openness, CM Documents, CM(2011)115-add1, 24 August 2011, § 80.

13 Czech Republic, Comments submitted by the Czech Republic in reaction to the initial "pre-draft" report of the Open-Ended Working Group on developments in the

referred to acts 'to the detriment of third parties'.[14] Asserting an arguably higher standard the Netherlands, Canada and Ecuador have referred to 'serious adverse consequences'[15], echoing Rule 6 of the Tallinn Manual which cumulatively referred to acts that 'affect the rights of, and produce serious adverse consequences for, other states'.[16] The Tallinn Manual however did not elaborate the basis of this threshold.[17] Scholarly statements on the application of international law in cyberspace have combined references to 'serious adverse consequences' and 'significant harm' and referred to 'significant adverse or harmful consequences'[18], indicating that both standards are closely related and that a meaningful differentiation between both cannot be made at this point. States may decide to apply a higher threshold of harm in cyberspace but the above-mentioned references are not sufficiently frequent and consistent to indicate that states want to apply a higher threshold than the predominant threshold of significant harm.

field of information and telecommunications in the context of international security, March/April 2020, p.3.

14 France, France's response to the pre-draft report from the OEWG Chair, March/April 2020, p. 4.

15 Netherlands, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, Appendix, International Law in Cyberspace, p. 5; Canada, Updated norms guidance text with additions from States, 30 November 2020, p. 2; Ecuador, Ecuador preliminary comments to the Chair's "Initial pre-draft" of the Report of the United Nations Open Ended Working Group on developments in the field of information and telecommunications in the context of international security (UN OEWG), April 2020, p. 2.

16 Schmitt, 'Tallinn Manual' (n. 1) 2017, rule 6, p. 30: 'A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.' The Tallinn Manual seemed to suggest that 'serious adverse consequences' is a higher threshold than 'significant' but did not elaborate why it chose this standard instead of the 'significance' standard. A reference to the Trail Smelter arbitration indicates that the Group of Experts may have derived the terminology from this award, see ibid. p. 37, para. 25.

17 Antonio Coco/Talita de Souza Dias, '"Cyber Due Diligence"': A Patchwork of Protective Obligations in International Law', *European Journal of International Law* 32 (2021), 771–805, at 786.

18 Oxford Institute for Ethics, Law and Armed Conflict (ELAC), Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research, 7 August 2020, para. 2, available at: https://elac.web.ox.ac.uk/article/the-second-oxford-statement#/. 'International law prohibits cyber operations by States that have significant adverse or harmful consequences(…)'.

Due diligence obligations are hence triggered by the risk of significant harm.[19] The ILC commentaries assert that the risk assessment is the 'combined assessment of the gravity/magnitude of harm and the probability of its occurrence'.[20] This combined assessment has been illustrated as two interconnected axes with sliding scale'.[21] The low probability of considerable harm as well as the high probability of minor harm will trigger preventive duties.[22] Assessing the probability-dependent assessment of a risk of significant harm has hence a predictive and future-oriented character.[23] The ILC commentaries refer to the 'appreciation of harm [that a properly informed observer] ought to have had'.[24]

The future-orientation of the risk assessment raises the question if beyond present or imminent risks of harm also general or abstract risks of harm[25] with yet unknown potential materialization and chains of causality trigger preventive duties.[26] In cyberspace, this aspect is particularly relevant as here the unpredictable behaviour of social groups, e.g. of cyber criminals or other non-state actors, is a particularly relevant risk scenario.[27]

19 ILC Draft Articles on Prevention (n. 6), art.1.

20 The ILC Draft Prevention articles refer to 'the combined effect of the probability of occurrence of an accident and the magnitude of its injurious impact'; ILC Draft Articles on Prevention (n. 6), commentary to art. 2, p. 152, para. 2.

21 Arie Trouwborst, *Precautionary Rights and Duties of States* (Leiden/Boston: Martinus Nijhoff 2006), 26.

22 See already ILC, Fifth Rep. on International Liability for Injurious Consequences Arising Out of Acts Not Prohibited by International Law, by Mr Julio Barboza, Special Rapporteur, A/CN.4/423; YBILC 1989, p. 85, para. 315.

23 ILC Draft Articles on Prevention (n. 6), commentary to art. 1, p. 151, para. 14: (14) As to the element of "risk", this is by definition concerned with future possibilities, and thus implies some element of assessment or appreciation of risk.'

24 Ibid.

25 The Tallinn Manual helpfully distinguishes between 'particularised' and 'general' risks in its discussion of the scope of the due diligence obligation but does not specify these types of risk further, Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), rule 7, p. 44, para. 7.

26 On the oversimplifying differentiation between known and unknown risks Stephen Townley, 'The Rise of Risk in International Law', *Chicago Journal of International Law* 18 (2018), 594–646, at 597: '"Unknown" risk is more inchoate potential peril about which we lack information either on the likelihood of the harm materializing or knowledge of the effect it would have if it did.'

27 On unpredictable human behaviour as a category of risk distinct from positive, scientifically accessible causality Heike Krieger/Anne Peters, 'Due Diligence and Structural Change in the International Legal Order', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 351–390, at 353.

A closer look at the harm prevention rule reveals that an exclusion of abstract or general risks from the scope of the harm prevention rule is not convincing. Already in the *Alabama* case the US Supreme Court linked due diligence to 'vigilance'.[28] Vigilance is *per definitionem* alertness with regard to possible, yet uncertain danger'.[29] Related to the continuity-entailing aspect of 'vigilance' it is furthermore acknowledged that due diligence is of a continuous character[30] – which only makes sense if already the existence of a general risk triggers the obligation to exercise due diligence. Furthermore, the ILC asserted that due diligence under the harm prevention rule may require to identify risky activities[31] which again logically presumes that already the existence of a general or abstract, yet in its materialization unknown risk suffices to trigger due diligence obligations. Lastly, a central due diligence requirement in general international law is taking legislative measures against risky activities.[32] As legislative measures overwhelmingly do not address particular risks requiring an instantaneous reaction but only anticipate general or abstract risks this also logically presumes that already general risks trigger due diligence obligations.

Therefore, an exclusion of abstract or general risks from the scope of the harm prevention rule is not plausible. The remoteness of the risk may duly

28 Tribunal of arbitration established by Article I of the Treaty of Washington of 8 May 1871, Alabama claims of the United States of America against Great Britain, Award of 14 September 1872, UNRIAA, XXIX, 125–134: '[A] diligence proportioned to the magnitude of the subject (…) a diligence which shall, by the use of active vigilance, and of all the other means in the power of the neutral, through all stages of the transaction, prevent its soil from being violated (…)'.

29 Robert Sprague/Sean Valentine, 'Due Diligence', Encyclopædia Britannica, 4 October 2018, available at: https://www.britannica.com/topic/due-diligence; see also Anne Peters/Heike Krieger/Leonhard Kreuzer, 'Due Diligence in International Law: Dissecting the Leitmotif of Current Accountability Debates', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 1–19, at 2.

30 Samantha Besson, 'La Due Diligence en Droit International', *Recueil des Cours de l'Académie de Droit International de la Haye* 409 (2020) 153–398, at 250, para. 197; CoE, Steering Committee on the Media and New Communication Services (CDMC), Explanatory Memorandum to the draft Recommendation CM/Rec (2011) of the Committee of Ministers to member states on the protection and promotion of Internet's universality, integrity and openness, CM(2011)115-add1 24 August 2011, para. 83: 'The commitment "to take all reasonable measures" to prevent and respond to disruptions or interference, or to minimise risks and consequences thereof, should be of a continuous nature.'

31 ILC Draft Articles on Prevention (n. 6), commentary to art. 3, p. 153, 154, para. 5.

32 Ibid., art. 5; see on required due diligence measures also chapter 4.D.I, II.

be considered in the interpretation of due diligence requirements which are proportionally diminished for unlikely or remote scenarios.[33] Furthermore, due diligence is not triggered by purely hypothetical or far-fetched scenarios.[34]

II. Integrating acts reaching the threshold of prohibitive rules into the risk of harm threshold

The editor of the Tallinn Manual has argued that in order for due diligence obligations to be triggered it does not suffice that a risk of significant (or serious) harm exists but that it is required that the harmful activity would amount to a violation of international law (if committed by a state).[35] Such an approach can point to the wording of para. 13 lit. c of the UN GGE Report 2015 – the harm prevention rule reference – that states must not allow 'internationally wrongful acts'.[36]

Such a high threshold is however hard to square with the case law of the harm prevention rule. The *Trail Smelter* merely required injurious consequences[37], the *Arjona* case a 'wrong' to another state.[38] The *Corfu Channel* and *Island of Palmas* case refer to 'rights'[39], but it is not evident that every interference with a right already constitutes an internationally wrongful act.[40] Furthermore, such a rigidly high threshold would significantly restrict the breadth of the rule's rationale. The open-endedness of the criterion of significant harm is a strength of the norm to also flexibly take new forms

33 Ibid., commentary to art. 3, p. 154, para. 11.
34 Ibid., commentary to art. 3, p. 153, 154, para. 5.
35 Michael Schmitt, 'Three International Law Rules for Responding Effectively to Hostile Cyber Operations', *JustSecurity*, 13 July 2021, available at: https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/: 'It must be cautioned that the rule does not apply to cyber operations unless they implicate the legal rights of other states (…) As noted above, the international law most likely to be breached by hostile cyber operations is sovereignty. Absent that rule, the due diligence obligation would apply only rarely.'
36 United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), A/70/174, 22 July 2015 (UN GGE Report 2015), para. 13 lit. c.
37 Trail Smelter' (n. 3), 1963.
38 US Supreme Court, United States v. Arjona, 7 March 1887, 120 U.S. Reports 1887, 484.
39 ICJ, 'Corfu Channel Case' (n. 3), p. 22; Arbitrator Max Huber, *Case of the Island of Palmas (Netherlands v. USA)*, Award of 4 April 1928, vol. II, UNRIIA, 829–871, 839.
40 Coco/Dias, 'Cyber Due Diligence' 2021 (n. 17), 785.

of harm into account.[41] In cyberspace, this benefit of the rule is particularly helpful as the question which low-level cyber harm violates international law is often not sufficiently clear.[42] It is hence preferable that the mere risk of significant harm triggers due diligence obligations to prevent[43] and that it is not necessary that an act amounts to a violation of a (distinct) rule of international law (if committed by a state).

Nevertheless, the discussion of when cyber operations reach the threshold of a prohibitive rule can also be made fruitful for the harm prevention rule. If an operation would reach the threshold of a prohibitive primary rule of international law if it was (hypothetically) conducted by a state this regularly indicates that the threshold of significant harm is met.[44] For example, if a cyber operation reaches the threshold of prohibited force, this will indicate the significance of harm. Hereby, acts which reach the threshold of prohibitive rules can be integrated into the preventive scope of the harm prevention rule. Such a 'hypothetical norm violation test' is important to close accountability gaps: It is often impossible to attribute malicious cyber activities to a state.[45] For example, if a single hacker, not associated in any way to a state, sabotages the IT system of a foreign parliament via ransomware – an act that may constitute prohibited intervention if committed by a state[46] – such a case would not fall under the prohibition of intervention as long as the attacker's acts are not attributable to the state.[47] Similarly, ransomware attacks on foreign hospitals by cyber criminals that may even amount to a prohibited use of force if committed by a state do not lead to a territorial state's accountability if the attack is not attributable to it. In such cases, the harm prevention rule enhances the territorial state's accountability by at least requiring it to prevent, stop or mitigate the harmful operation.

It is important to note that integrating acts reaching the threshold of prohibitive rules into the scope of the harm prevention rule via a 'hypothetical norm violation test' in no way bears on the question of legal consequences

41 Crootof, 'International Cybertorts' 2018 (n. 9), 608.
42 See Introduction.
43 A fortiori the negative prohibitive dimension of the harm prevention rule obliges states not to cause such harm trough own acts. On the negative prohibitive dimension of the rule see chapter 2.A.VI.
44 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), p. 34, para. 15.
45 See Introduction.
46 See below chapter 3.B.II.2.3.2.
47 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 66, p. 313, 314, para. 4.

on the secondary level. The legal consequences of a violation of the harm prevention rule remain exclusively determined by the rules applicable to a violation of the harm prevention rule. States are only entitled to take non-forcible countermeasures against a violation.[48] Utilizing the prohibitive threshold as an indicator for significant harm hence by no means leads to the applicability of secondary rules applicable to the violation of such prohibitive rules[49] through the backdoor.

III. Interpretation of risk of significant harm in cyberspace

Beyond acts reaching the threshold of prohibitive rules it is highly abstract which cyber harm is considered 'significant' harm. Due to the criteria's inherent context-dependent subjectiveness[50] it needs interpretative specification by states.[51] *Jolley* suggested to look at the 'scale and effects on the state as a whole'.[52] Similarly, the UN GGE Report 2021 referred to the scale and seriousness of an attack to assess its gravity.[53] *Schmitt* has suggested that the threshold may be reached when the harm has become a 'concern in inter-state relations'.[54] *Walton* has pointed out that the threshold of

48 On legal consequences of a violation of the harm prevention rule see chapter 5.C.I.

49 E.g. the right to self-defence against prohibited force that may amount to armed attack under Art. 51 UN Charter.

50 Coco/Dias, 'Cyber Due Diligence' 2021 (n. 17), 793: 'The determination of what amounts to significant harm involves a subjective assessment that varies depending on the circumstances prevailing at the time'.

51 Crootof, 'International Cybertorts' 2018 (n. 9), 608: 'States, like plaintiffs in domestic law, will determine what injuries they will absorb and which are worth challenging; other states' responses to such accusations will be instrumental in developing norms about what constitutes significant harm'.

52 Jason D. Jolley, *Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law* (University of Glasgow 2017), 190.

53 On the merits of classifying cyber incidents in terms of scale and seriousness United Nations, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UN GGE), A/76/135, 14 July 2021 (UN GGE Report 2021), para. 50. Although the criteria are proposed regarding cyber harm to critical infrastructure they seem similarly suitable for assessing the significance of cyber harm generally.

54 Michael N. Schmitt, 'In Defense of Due Diligence in Cyberspace', *Yale Law Journal Forum* 125 (2015), 68–81, at 76; see also Zine Homburger, 'Recommendation 13a', in Eneken Tikk (ed.) *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary,* (United Nations Office for Disarmament Affairs 2017), 9–25, at 16, para. 15.

significant harm may also be assessed with a view to a state's duty to protect under international human rights law.[55]

All suggestions have their own merits and may serve as reference points for the context-dependent assessment of significant harm. With regard to the latter suggestion there is indeed an overlap of the protective scope of the harm prevention rule with that of human rights law.[56] Yet, the protective scope of the harm prevention rule is broader as it also covers harm on the societal level beyond harm to individual rights. Hence, exclusively focussing on the protective scope of human rights law would overly restrict the protective scope of the harm prevention rule. In line with the flexible sliding scale characteristic of the determination of the risk of transboundary harm[57] it seems important to firstly assess the quantitative and qualitative effects of cyber harm[58] and to secondly enquire whether this leads to a 'concern in inter-state relations'. Indeed, protests by states, legal statements and in general assertions of opinio iuris[59] are the strongest indicator that the threshold of significance has been met. However, a certain ambiguity in the evolutionary process towards specification of the abstract term significant harm is admittedly inevitable.

IV. Non-physical harm as relevant harm under the harm prevention rule

As cyber harm can be both physical as well as non-physical[60] it needs to be enquired whether harm needs to amount to physical harm in order to be

55 Assuming that harm beyond the scope of the duty to protect is covered under the harm harm rule, yet pointing at the difficulty of assessing it Beatrice A. Walton, 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law', *Yale Law Journal* 126 (2017), 1460–1519, at 1507.

56 In more detail on the overlap and divergence regarding the protective scope of the due diligence requirement under duty to protect in international human rights law and the due diligence requirement under the harm prevention rule see chapter 4.B.III.

57 See Trouwborst, 'Precautionary Rights and Duties' 2006 (n. 21), 26.

58 This could be the gravity of cyber harm-induced loss of confidentiality, loss of functionality or physical damage. See on these three categories of cyber harm effects chapter 1.C. Also arguing for quantitative and qualitative criteria to assess the gravity of cyber harm Harriet Moynihan, 'The Application of International Law to State Cyberattacks Sovereignty and Non-intervention', *Chatham House – Research Paper*, 2019, para. 158. She makes the argument in the context of a potential sovereignty rule but the considerations equally apply to the harm prevention rule.

59 See above chapter 2.D.V.

60 See chapter 1.C.

considered significant harm. The ILC notably limited its Draft Articles on Prevention, after initial discussions on a wider scope, to physical harm and excluded non-physical harm to make the articles more manageable.[61]

However, during the drafting process states indicated that they found the limitation to physical harm too restrictive.[62] Also an ILC study during the drafting process pointed at state practice that considered non-physical (or in the study: 'non-material') harm as relevant harm, e.g. in international telecommunications law under the Constitution of the International Telecommunications Union (ITU)[63] or the ITU Radio Regulations.[64] Also an ILC Survey assumed that the rules of the ILC project may also apply to non-physical harm, pointing to examples in broadcasting and airspace.[65] Other commentators have furthermore shown that the harm prevention rule also applies in the field of international economic law, e.g in banking law, tax law, or currency law.[66]

---

61 ILC Draft Articles on Prevention (n. 6), art.1: 'The present articles apply to activities not prohibited by international law which involve a risk of causing significant transboundary harm through their physical consequences.' On the evolution of the discussion in the ILC Bäumler, 'Schädigungsverbot' 2017 (n. 2), 64f.

62 ILC, International liability for injurious consequences arising out of acts not prohibited by international law (Prevention of transboundary damage from hazardous activities), A/CN.4/509, Comments and observations received from Governments: report of the Secretary-General, 17 April 2000, comments by the Netherlands, p. 131, para. 1: 'While acknowledging the desirability of keeping the scope of the articles manageable, which is why the formulation "physical consequences" has been adopted, the Netherlands nonetheless doubts whether the term "physical" is broad enough for this purpose'.

63 International Telecommunication Union, Constitution and Convention of the International Telecommunication Union, 1 July 1994, UNTS 1825, 1826, art. 45.

64 International Telecommunication Union, Radio Regulations, 22 December 1992, para. 4.8, para. 4.10.

65 ILC, "International Liability for Injurious Consequences Arising Out of Acts Not Prohibited by International Law": Survey Prepared by the Secretariat, A/CN.4/471, YBILC 1995, at 61. The International Radiotelegraph Convention for example requires states to operate stations in a way that does not interfere with the radioelectric communications of other state parties or of persons authorized by those Government, International Radiotelegraph Convention of Washington, 25 November 1927, art. 10 (2): 'stations, whatever their object may be, must, so far as possible, be established and operated in such manner as not to interfere with the radioelectric communications or services of other contracting Governments and of individual persons or private enterprises authorized by those contracting Governments to conduct a public radiocommunication service.' See also Walton, 'Duties Owed' 2017 (n. 55), 1482, fn. 114.

66 Jelena Bäumler, 2017, 'Implementing the No Harm Principle in International Economic Law: A Comparison between Measure-Based Rules and Effect-Based Rules', *Journal of International Economic Law* 20 (2017), 807–828; Markus Krajewski, 'Due Dili-

This strongly suggests that the harm prevention rule may also include non-physical harm as significant harm. Regarding cyberspace, states and commentators seem to concur with this view. For example, the Netherlands has stated explicitly that also non-physical harm is relevant under the harm prevention rule in cyberspace.[67] Similarly, Germany has argued for the relevance of non-physical cyber harm.[68] Also assertions of content harm as relevant harm by more authoritarian states similarly indicate a broad understanding of significant harm which includes non-physical harm.[69] Additionally, several commentators have argued for the inclusion of non-physical harm as significant harm[70] and have e.g. conceived disinformation as relevant harm under the rule.[71]

Therefore, while more opinio iuris on the inclusion of non-physical harm under the harm prevention rule would be desirable, it seems unconvincing to exclude non-physical harm from its scope. Indeed, cyber harm

gence in International Trade Law', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 312–328.

67 Netherlands, 'International Law in Cyberspace' 2019 (n. 15), p. 5.

68 In the context of a potential sovereignty rule in cyberspace Germany, On the Application of International Law in Cyberspace, March 2021, p. 3, 4: 'Germany generally also concurs with the view expressed and discussed in the Tallinn Manual 2.0 that certain effects in form of functional impairments with regard to cyber infrastructures located in a State's territory may constitute a violation of a State's territorial sovereignty. In Germany's view, this may also apply to certain substantial non-physical (i.e. software-related) functional impairments. In such situations, an evaluation of all relevant circumstances of the individual case will be necessary.'

69 Iran, Zero draft report of the Open-ended working group On developments in the field of information and telecommunications in the context of international security, UN OEWG, January 2021, p. 13: 'States should ensure appropriate measures with a view to making private sector with extraterritorial impacts, including platforms, accountable for their behaviour in the ITC environment. States must exercise due control over ICT companies and platforms under their (…) jurisdiction, otherwise they are responsible for knowingly violating national sovereignty, security and public order of other states' It may be problematic to develop sufficiently ascertainable legal criteria regarding content harm.

70 Katharina Ziolkowski, 'General Principles of International Law as Applicable in Cyberspace' in Katharina Ziolkowski (ed.) *Peacetime Regime for State Activities in Cyberspace* (NATO CCDCOE 2013), 135–188, at 166: Walton, 'Duties Owed' 2017 (n. 55), 1505; Coco/Dias, 'Cyber Due Diligence' 2021 (n. 17), 793; Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 6, p. 37, para. 28.

71 Marko Milanovic/Michael Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations during a Pandemic', *Journal of National Security Law & Policy* 11 (2020) 247–284, at 280.

is frequently non-physical and occurs only ICT-internal, e.g. leading to loss of confidentiality or loss of functionality.[72] Excluding such harm from the scope of the harm prevention rule would drastically reduce the rule's practical relevance.

V. Cumulative harm as relevant harm under the harm prevention rule

The *Trail Smelter* arbitration indicates that the significance threshold can also be achieved through the cumulative effect of different 'smaller' harms over prolonged periods of time. In assessing the harm caused by the fumes of the trail smelter the tribunal analysed the time periods during which harming fumes were emitted to conclude that the threshold of serious harm was achieved inter alia due to the duration of the occurring harm.[73]

This is relevant for the cyber context: A single instance of cyber harm as such may not suffice to be considered of concern in inter-state relations or significant in its quantitative and qualitative effects. For example, a single ransomware attack against a business in state A emanating from state B may as such not trigger preventive duties. However, a large number of ransomware attacks over an extended period of time, causing increasing quantitative costs over time may reach the threshold. The US has asserted that cumulative costs of cyber harm may affect national security.[74] Australia has explicitly highlighted that the cumulative cyber harm may endanger international peace and security.[75] A certain openness regarding the time-

72 See chapter I.C.I, II.

73 Trail Smelter' (n. 3), at 1926, 1927: '(…) the Tribunal has found that damage due to fumigation has occurred to trees during the years 1932 to 1937 inclusive, in varying degrees, over areas varying not only from year to year but also from species to species (…) It is uncontroverted that heavy fumigations from the Trail Smelter which destroyed and injured trees occurred in 1930 and 1931 and there were also serious fumigations in earlier years'.

74 US Director of National Intelligence, James Clapper, Statement for the Record, Worldwide Cyber Threats 10 September 2015: '(…) the likelihood of a catastrophic attack from any particular actor is remote at this time. Rather than a "Cyber Armageddon" scenario that debilitates the entire US infrastructure, we envision something different. We foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security'.

75 Australia's International Cyber Engagement Strategy, October 2017, p. 45: '(…) international peace, security and stability could be (…) threatened by the cumulative effect of repeated low-level malicious online behaviour.'

frame for assessing the significance of cyber harm has hence been acknowledged. The concept of cumulative cyber harm can be made fruitful to assess the effects of recurring cyber operations, such as the gradual erosion of public trust in public institutions, or gradually rising small-scale economic harm.[76]

VI. Context-dependent flexible assessment of significant cyber harm

Overall, the determination of a risk of significant cyber harm hence requires a context-dependent flexible assessment. To sum up: Due diligence obligations to prevent and mitigate are triggered by the risk of significant cyber harm. Also abstract risks of cyber harm, as well as risks of non-physical cyber harm, may amount to a risk of significant cyber harm. The significance of a risk of cyber harm may also be achieved through cumulative effects over a prolongued period of time. Decisive is whether a risk of harm amounts to a concern in inter-state relations. If an act reaches the threshold of a prohibitive rule of international law, this regularly indicates that the threshold of a risk of significant harm is met. Reaching such a threshold is however not necessary for assuming a risk of significant cyber harm.

To flesh out emerging cyber harm risk thresholds the study will in the following first analyse which risks of cyber harm reach the threshold of a prohibitive rule of international law (B.). In a second step, it will analyse which risks of cyber harm have become a 'concern in inter-state relations' due to their quantitative or qualitative effects (C.).

B. Acts reaching the threshold of prohibitive rules

The fact that a cyber operation would amount to an internationally wrongful act if it had been committed by a state indicates that the threshold of significant harm is reached. Under this 'hypothetical norm violation test'[77] it is notably not necessary that the act was indeed conducted by a state. It is sufficient that the conduct would have been prohibited and hence internationally wrongful if it had hypothetically been committed by a state.

76 On harmful cyber espionage operations against governmental and international institutions see chapter 3.C.IV.

77 On the 'hypothetical norm violation test' as an indicative benchmark for the question whether a risk of significant harm exists see above chapter 3.A.II.

Hereby non-attributable acts of non-state actors that would otherwise not be grasped by international law come into the realm of international law.

I. Prohibition on the use of force

Cyber harm can lead to effects that would – if the act had been committed by a state – constitute a violation of the prohibition on the use of force. The prohibition on the use of force is the cornerstone rule protecting international peace and security.[78]

1. Recognition of the prohibition on the use of force in cyberspace

Under which circumstances a malicious cyber operation amounts to a use of force has been discussed extensively in the 'cyberwar' debate[79] and the Tallinn Manual.[80] States have endorsed the prohibition on the use of force in cyberspace, e.g. in the UN GGE[81], the UN General Assembly[82], national

78 Art. 2 (4) UN Charter: 'All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.'; Oliver Dörr, 'Prohibition of Use of Force', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2019), para. 1.

79 See for the extensive discussion e.g. Johann-Christoph Woltag, *Cyber Warfare* (Intersentia 2014); Martin C. Libicki, 'Cyberspace is not a Warfighting Domain', *I/S: A Journal of Law and Policy for the Information Society* 8 (2012), 321–336; Nils Melzer, *Cyberwarfare and International Law* (United Nations Institute for Disarmament Research, Ideas for Peace and Security-Resources 2011); Marco Roscini *Cyber operations and the use of force in international law* (Oxford: Oxford University Press 2014).

80 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), Rule 68–70.

81 UN GGE Report 2021, para. 70d; UN GGE Report 2015, para. 26.

82 UN General Assembly Resolution A/RES/75/240, 31 December 2020: 'Recalling that (…) the Group of Governmental Experts (…) identified as of central importance the commitments of States to (…) refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State'.

strategy documents[83] or statements[84], and statements in the UN OEWG.[85] When states have pushed back against the prohibition they have done so out of the concern about an alleged militarization or weaponization[86] of cyberspace and an abuse of the right to self-defence following a cyber operation.[87] Guyana has for example opined that a cyber operation 'by itself may not constitute a use of force' as no 'physical weaponry' is involved – hereby seemingly pushing back against mere ICT-internal harm as a use of force. Such positions however do not categorically exclude the possibility that the causation of physical or ICT-external harm via cyber means could constitute a use of force.

83 See e.g. Japan, Basic Position of the Government of Japan on International Law Applicable to Cyber Operations, 28 May 2021, p. 5: 'The obligation to refrain from the threat or use of force in international relations is an important obligation relating to cyber operations.'

84 Organization of American States, Improving Transparency — International Law and State Cyber Operations: Fourth Report (Presented by Prof. Duncan B. Hollis), CJI/doc. 603/20 rev.1 corr.1, 5 March 2020, para.23.'

85 UK, Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015., September 2019, p.2; Australia, Australian Comments on Zero draft 22 February 2021, para 19; UN OEWG, Zero Draft, para. 28. In the UN OEWG Final Report the reference was omitted which is striking, given its nearl universal endorsed by states. Yet, the omission is to be seen in the context of the sparsity of the UN OEWG Final Report on international law. At least an indirect reference may be deduced from the assertion that staes are called upon to 'avoid and refrain from taking any measures not in accordance with international law, and in particular the Chapter of the United Nations' UN OEWG Final Report 2021, para. 34.

86 Iran, Open-ended working group on: Developments in the field of information and telecommunications in the context of international security Submission by the Islamic Republic of Iran, September 2019, para. 11: 'ICT environment is prone to weaponization if and when designed or used to inflict damage on the infrastructures of a State.'

87 Organization of American States, Improving Transparency — International Law and State Cyber Operations: Fourth Report (Presented by Prof. Duncan B. Hollis), CJI/doc. 603/20 rev.1 corr.1, 5 March 2020, para. 25: '(…) Guyana's response expressed doubts about the applicability of the jus ad bellum to cyber operations alone. Relying on Black's Law Dictionary for a definition of force as "power dynamically considered," Guyana indicated that a cyber operation "by itself may not constitute a use of force." Similarly, it defined an armed attack as involving "weaponry" and to the extent "no physical weaponry is involved" in a cyber operation, it may not be considered an armed attack triggering selfdefense'.

2. Acts amounting to a use of force in cyberspace

Which cyber operations amount to prohibited force is not fully clear. In principle, the use of force should be interpreted restrictively as an extensive interpretation risks to trigger a right to self-defence as *ultima ratio* too quickly.[88]

What amounts to a use of force is generally assessed by reference to the scale and effects criterion asserted by the ICJ in its *Nicaragua* judgment.[89] According to this standard an operation constitutes a prohibited use of force when it is comparable in its scale and effects to the kinetic effects of a traditional military operation. In cyberspace, states have largely endorsed the scale and effects threshold, e.g. Australia, Germany, and several states in the OAS.[90] When a cyber operation is comparable to a traditional kinetic military operation in its scale and effects however needs specification.[91]

88 Finland, 'International law and cyberspace' 2020 (n. 10), p. 7: 'Any interpretation of the use of force in cyberspace should respect the UN Charter and not just the letter of the Charter but also its object and purpose, which is to prevent the escalation of armed activities.

89 ICJ, *Military Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment of 27 June 1986, ICJ Reports 1986, p. 14, 103, para. 195: '(…) in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces.'

90 See for an overview Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views ', *The Hague Programe for Cyber Norms – A Policy Brief,* March 2020, p. 9; Australia, Australian Paper – Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International security, September 2019: 'In determining whether a cyber attack, or any other cyber activity, constitutes a use of force, states should consider whether the activity's scale and effects are comparable to traditional kinetic operations that rise to the level of use of force under international law; OAS, 'Improving Transparency – 4th Report' 2020 (n. 84), para. 26: 'Most responding States continue to find power in drawing the relevant thresholds by analogizing cyber operations to kinetic or other past operations that did (or did not) qualify as a use of force or armed attack'.

91 UN OEWG, Zero Draft, para. 34; Antonio Segura-Serrano, 'The Challenge of Global Cybersecurity', in: Antonio Segura-Serrano (ed.), *Global Cybersecurity and International Law* (Routledge 2024), 1–9, at 2; highlighting uncertainty regarding economic coercion as a use of force Christine Gray, 'The prohibition of the use of force', in *International Law and the Use of Force* (4th ed 2012), p. 33.

The most extensive approaches have gone so far as to view the mere alteration of data as prohibited force[92] which has however rightly been refuted.[93] France has put forward a similarly extensive argument that 'penetrating military systems in order to compromise defence capabilities' may constitute prohibited force.[94] This arguably suggests that even cyber espionage operations may constitute a use of force. However, as cyber espionage operations are widely practiced in international relations, including against military institutions, such an extensive interpretation would lead to a permanent existence of a right to self-defence and hereby largely hollow out the prohibition on the use of force.[95] This would run counter to the object and purpose of the UN Charter, 'which is to prevent the escalation of armed activities'.[96] Even if acts of cyber espionage may be called 'acts of war' in the political discourse[97], such assertions seem politically motivated and legally hardly justifiable.

The Netherlands have asserted that a cyber operation leading to 'serious financial or economic impact' may constitute a use of force.[98] Causing economic harm was however excluded from the prohibition on the use force for good reasons.[99] While it is still discussed if it is necessary that use

92 Alexander Melnitzky, 'Defending America against Chinese Cyber Espionage Though the Use of Active Defences', *Cardozo Journal of International and Comparative Law* 20 (2012), 537–570, at 538, 564.

93 See e.g. Henning Lahmann/Robin Geiß, 'Freedom and Security in Cyberspace: Non-Forcible Countermeasures and Collective Threat-Prevention', in Katharina Ziolkowski (ed.) *Peacetime Regime for State Activities in Cyberspace* (NATO CCDCOE 2013), 621–657, at 623.

94 France, International Law Applies to Operations in Cyberspace, September 2019, p. 7.

95 Leonhard Kreuzer, 'Hobbesscher Naturzustand im Cyberspace? Enge Grenzen der Völkerrechtsdurchsetzung bei Cyberangriffen', in Ines-Jacqueline Werkner/Niklas Schörnig (eds.), *Cyberwar – die Digitalisierung der Kriegsführung* (Wiesbaden: Springer 2019), 63–86, at 68.

96 Finland, 'International law and cyberspace' 2020 (n. 10), p. 7.

97 Yevgeny Vindman, 'Is the SolarWinds Cyberattack an Act of War? It Is, If the United States Says It Is', *JustSecurity*, 26 January 2021, available at: https://www.lawfareblog.com/solarwinds-cyberattack-act-war-it-if-united-states-says-it; see Jan Wolfe/Brendan Pearson, 'Explainer-U.S. government hack: espionage or act of war?', *Reuters,* 19 December 2020.

98 Netherlands, 'International Law in Cyberspace' 2019 (n. 15), p. 4, open in this regard Finland, 'International law and cyberspace' 2020 (n. 10), p. 6.

99 Arguing for the exclusion of economic coercion from the use of force, inter alia based on the travaux preparatoir of the UN Charter Dörr, 'Use of Force' 2019 (n. 78), paras. 11, 12.

of force requires physical harm[100], aligning economic harm as comparable to a kinetic military operation clearly overstretches the notion of scale and effects. Notably, even its legal evaluation as coercion under the prohibition of intervention is contested.[101] In a tightly interconnected economic international order it may have dangerous destabilizing consequences beyond cyberspace to elevate cyber-enabled economic harm to prohibited force.

The most prevailing interpretation is that comparability exists in cases of death or injury of persons, or significant or serious damage to an object.[102] This position has e.g. been asserted by the UK[103], Australia[104], the AU[105], or Iran.[106] In particular physical damage to critical infrastructure may indi-

100 Olivier Corten, *The Law against War – The Prohibition on the Use of Force in Contemporary International Law* (Oxford: Hart Publishing 2010), 50; Tom Ruys, 'The Meaning of Force and the Boundaries of the *Jus ad Bellum*', *American Journal of International Law* 108 (2014) 159–210.

101 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 66, p.324, para. 35.

102 See for an overview Roguski, 'Comparative Analysis' 2020 (n. 90), at 10; see also Heike Krieger, 'Conceptualizing Cyberwar, Changing the Law by Imagining Extreme Conditions?', in Thomas Eger/Stefan Oeter/Stefan Voigt (eds), *International Law and the Rule of Law under Extreme Conditions: An Economic Perspective* (Tübingen: Mohr Siebeck 2017), 195–212, at 205, 206: 'The requirements of effects comparable to kinetic weapons – in particular immediacy, directness and a certain gravity of the attack, as well as a high burden of proof – guarantee that the international community has a reasonably secure basis for evaluating the state's legal claim.'

103 UK Attorney General Wright, Cyber and International Law in the 21st Century, Speech 23 May 2018: '(…) the UK considers it is clear that cyber operations that result in, or present an imminent threat of, death and destruction on an equivalent scale to an armed attack will give rise to an inherent right to take action in self-defence, as recognised in Article 51 of the UN Charter. (…)'.

104 Australia, 'Australian Paper' 2019 (n. 90), Annex A, p. 5: 'This involves a consideration of the intended or reasonably expected direct and indirect consequences of the cyber attack, including for example whether the cyber activity could reasonably be expected to cause serious or extensive ('scale') damage or destruction ('effects') to life, or injury or death to persons, or result in damage to the victim state's objects, critical infrastructure and/or functioning'.

105 African Union, Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, 29 January 2024 (endorsed by the Assembly of the AU on 18 February 2024), para. 40: '(…) a cyber operation that destroys, inflicts damage, or permanently disables critical infrastructure or civilian objects within a state may be considered (…) a use of force (…)'.

106 Iran, Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace, July 2020, article IV: '(…) certainly, those cyber operations resulting in material damage to property

cate that the threshold of prohibited force is met.[107] For example, cyber operations which affect medical treatment or water can potentially cause injury, death or extensive physical damage. Due to the sparse specification states are well-advised to further specify the criteria of a use of force.[108] In this regard they may take into account the abstract criteria that have been suggested by the Tallinn Manual.[109] These criteria so far do not reflect state practice or opinio iuris but rather entail a predictive element.[110] Assertions that significantly lower the threshold for a use of force, e.g. by also including non-physical financial harm, or via embracing a cumulative events doctrine, would in any case run counter to the restrictive interpretation required for the interpretation of Art. 2 (4) UN Charter.

At present, scale and effects comparability can hence only be assumed in cases of death and injury to individual and serious damage. This means that ICT-internal harm (loss of confidentiality, loss of functionality) as such cannot be considered a prohibited use of force. Only the occurrence of sufficiently causally linked physical damage to objects or persons – ICT-external harm[111] – can be the basis for the conclusion that a cyber operation rose to the level of prohibited force.

---

and/or persons in the widespread and grave manner (…) (sic) (…) constitutes use of force.'

107 Ibid., art. IV; Australia, 'Australian Paper' 2019 (n. 90), Annex A, p. 5; François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press 2020), 298.

108 See in this vein also UN OEWG Final Report 2021, para. 34: 'States also concluded that further common understandings need to be developed on how international law applies to State use of ICTs'.

109 The Tallinn Manual proposed the criteria severity, immediacy, directness, invasiveness, measurability, military character, state involvement, see Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 68, p. 334–336, para. 9. The reception of states of these very broad criteria has so far been reluctant. States have at best endorsed only some of the criteria, see e.g. the endorsement of Germany of the criteria of immediacy and military character; Germany, 'Security as a Dimension of Security Policy" – Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, at Chatham House, 18 May 2015, '(…) Factors to be taken into account include, inter alia, the seriousness of the attack, the immediacy of its effects, depth of penetration of the cyber infrastructure and its military character.'

110 Critical on the anticipatory methodology of the Tallinn Manual Krieger, 'Conceptualizing Cyberwar' 2014 (n. 102), 201.

111 On different degrees of cyber harm see chapter 1.C.

3. Application of the threshold to specific cyber incidents

Applying this threshold to historical cases shows that already a few cyber operations constituted a prohibited use of force. For example, in the so-called *Stuxnet* attack on Iran in 2010 malware spread via a simple USB stick led to the self-destruction of nuclear centrifuges in an Iranian nuclear facility. The precise physical damage is unknown but it is clear that an explosion of the centrifuges could easily have led to severe injuries, loss of life or substantial physical damage. The *Stuxnet* attack is hence widely considered as likely crossing the threshold of prohibited force, or at least presenting a borderline case.[112]

The cyber operation against the Iranian Nuclear Natanz Facility in April 2021, presumably by Israel, which disabled its electricity grid likely occurred to coerce Iran to stop its nuclear enrichment project.[113] Due to explosions in the facility the substantial damage likely crossed the threshold of prohibited force. Also the cyber operation *Black Energy* against three Ukrainian electricity providers presumably crossed the threshold. The cyber operation led to the regional interruption of electricity supply for up to six hours. Although injuries or lethal effects of the attack are not known the fact that such damages could potentially occur seem plausible. A further example is the *WannaCry* attack in 2017 which paralyzed inter alia hospitals and ongoing medical treatments. Although no lethal effects are known at least the delayed treatment of patients in medical need may be considered an injury and hereby cross the threshold to prohibited force. In September 2020 a cyber operation targetting a German hospital led to the delayed treatment of a woman who subsequently died.[114] Although this was presumably an accidental side effect of a cybercrime operation by non-state actors, also such an attack – if it had been committed by a state or been attributable

112 Henning Christian Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge: Cambridge University Press 2020), at 64.

113 Maziar Motamedi 'Iran calls blackout at Natanz atomic site 'nuclear terrorism", *Al Jazeera,* 11 April 2021, available at: https://www.aljazeera.com/news/2021/4/11/incident-at-iranian-nuclear-site-targeted-by-blast-last-year; Patrick Kingsley/David E. Sanger/Farnaz Fassihi, 'After Nuclear Site Blackout, Thunder From Iran, and Silence From U.S.', *New York Times*, 27 August 2021, available at: https://www.nytimes.com/2021/04/12/world/middleeast/iran-israel-nuclear-site.html.

114 Mellisa Eddy/Nicole Pelroth,'Cyber Attack Suspected in German Woman's Death', *New York Times*, 18 September 2020, available at: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.

to it – would have amounted to a prohibited use of force. By contrast, other operations, while severe in their effects, such as the *SolarWinds* operation, or the hack of the German Bundestag, can solely be characterized as cyber espionage and clearly fall short of the threshold of prohibited force as the effects remained limited to ICT-internal, non-destructive effects.

Hence, overall, a number of cyber operations have amounted to a prohibited use of force and hence triggered due diligence obligations to prevent, regardless of whether the acts were conducted by state or non-state actors. The overwhelming majority of cyber operations has however not crossed this threshold.

It is noteworthy that even in cases where the threshold was met states have been reluctant to invoke a violation of the use of force or to call out an armed attack. In none of the cases states protested or alleged a use of force or asserted a right to act in self-defence. For example, in April 2021, Iran referred to 'nuclear terrorism' and 'sabotage' and vowed 'revenge[115]' but did neither specify who was responsible for the attack nor invoked a right to self-defence. With regard to the *NotPetya* attacks against Ukraine the UK merely criticized 'continued disregard for sovereignty'.[116] Such reluctance concurs with the general reluctance regarding reactions to cyber operations[117], in particular the reluctance to resort to countermeasures, and the preference to react with diplomatic protests and covert operations.[118] This shows that the frequently asserted right to self-defence against cyber operations is part of states' deterrence portfolio but has little practical relevance so far.

115 Kingsley/Sanger/Fassihi, 'Thunder From Iran' (n.113).

116 UK, National Cyber Security Center, Russian military 'almost certainly' responsible for destructive 2017 cyber attack', 14 February 2018, 'The UK Government judges that the Russian Government, specifically the Russian military, was responsible for the destructive NotPetya cyber-attack of June 2017 (…) The attack showed a continued disregard for Ukrainian sovereignty (…) We call upon Russia to be the responsible member of the international community it claims to be rather then secretly trying to undermine it'.

117 See Introduction.

118 Dan Efrony/Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber-operations and Subsequent State Practice', *The American Journal of International Law* 112 (2018), 583–657, at 654: '[A]t this point in time, states seem to prefer to engage in cyberoperations and counteroperations "below the radar," and to retain, for the time being, some degree of stability in cyberspace by developing "parallel tracks" of restricted attacks, covert retaliation, and overt retorsion, subject to certain notions of proportionality.'

4. The exceptional implication of the threshold of prohibited force in cyberspace

Although cyber war is a persistently looming threat scenario in the public discourse such a cyber war has so far not taken place. Cyber operations will amount to a use of force only in highly exceptional circumstances.[119] According to the preferable restrictive interpretation the risk of a prohibited use of force can be assumed only if there is a risk of cyber harm that causes death or injury or substantial physical damage. In this case due diligence obligations to prevent are triggered, regardless of whether the harmful act is attributable to a state.

II. Prohibition of intervention

Cyber operations may also reach the threshold of a prohibited intervention or interference in the internal or external affairs of a state.

1. Recognition of the prohibition of intervention in cyberspace

Numerous states and commentators[120] have asserted the application of the prohibition in cyberspace, e.g. in the UN GGE Report[121], and in individual statements.[122] No state has objected to its applicability in cyberspace. Like the prohibition of the use of force the prohibition of intervention in the

119 Germany, 'Application of International Law' (n. 68), p. 6: 'So far, the vast majority of malicious cyber operations fall outside the scope of 'force''.

120 Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions', *Journal of Conflict & Security Law* 17 (2012), 211–227; Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), rule 66; Terry D. Gill, 'Non-intervention in the Cyber Context', in Katharina Ziolkowski (ed.) *Peacetime Regime for State Activities in Cyberspace* (NATO CCDCOE 2013), 217–238; Moynihan, 'The Application of International Law' 2019 (n. 58).

121 UN GGE Report 2015, para. 28 lit. b; UN GGE Report 2021, paras. 70, 71c.

122 E.g. China, International Strategy of Cooperation on Cyberspace, 2016: 'No country should pursue cyber hegemony, interfere in other countries' internal affairs, or engage in, condone or support cyber activities that undermine other countries' national security. No country should pursue cyber hegemony, interfere in other countries' internal affairs, or engage in, condone or support cyber activities that undermine other countries' national security'.

internal affairs of a state is a fundamental duty[123] of states and has been described by the ICJ as 'part and parcel' of international law.[124] In the quest for a norm against low-level cyber harm the norm has featured prominently in discussions and many commentators have focussed on interpreting the rule[125] as it has increasingly become clear that the use of force threshold will regularly not be met.

The Friendly Relations Declaration of the UN General Assembly expresses the rule's core rationale:

> 'No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.'[126]

The ICJ specified the two constituent elements of the norm in its *Nicaragua* judgment:

> '[i]ntervention is wrongful when it uses methods of coercion in regard to such choices [of a political, economic, social and cultural system, and the formulation of foreign policy], which must remain free ones. The element of coercion which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State.'[127]

123 Philip Kunig, 'Prohibition of Intervention' in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2008), para. 7.

124 ICJ, 'Nicaragua' (n. 89), para. 202.

125 See Michael P. Fischerkeller, 'Current International Law Is Not an Adequate Regime for Cyberspace', *LawfareBlog*, 22 April 2021, available at: https://www.lawfareblog.com/current-international-law-not-adequate-regime-cyberspace; Ido Kilovaty, 'The Elephant in the Room: Coercion', *AJIL Unbound* 113 (2019), 87–91; Gary Corn, 'Covert Deception, Strategic Fraud, and the Rule of Prohibited Intervention', *LawfareBlog*, 24 September 2020, available at: https://www.lawfareblog.com/covert-deception-strategic-fraud-and-rule-prohibited-intervention.

126 UN, General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, A/RES/25/2625, 24 October 1970.

127 ICJ, 'Nicaragua' (n. 89), para. 205.

Characteristic for a prohibited intervention is hence an impact on central governmental policy choices (domaine réservé) that is coercive.[128] States have largely endorsed both constituent elements (domaine réservé and coercion) in cyberspace.[129]

2. Domaine réservé

Regarding the first element – the domaine réservé – a precise definition does not exist. The ICJ dictum in *Nicaragua* referred to 'choices of a political, economic, social and cultural system, and the formulation of foreign policy'.[130] Negatively circumscribed the domaine réservé is an area that is the exclusive domain of sovereign states and secluded from the international sphere. In an increasingly interconnected inter-state sphere the realm of domestic spheres entirely secluded from the international sphere is shrinking[131] which is particularly relevant in the interconnected cyberspace. Regulatory choices e.g. regarding the level of data security and e-commerce have usually international ramifications. Nevertheless, it seems important that key policy choices would still be considered protected by the prohibition of intervention and hence falling within the domaine réservé, as they essentially concern the territorial state's exclusive prescriptive and

128 On the centrality of the coercive element for the norm see Benedikt Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace', in: Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace* (NATO CCDCOE 2013), 189–216.

129 For an overview Roguski, 'Comparative Analysis' 2020 (n. 90), p. 8; Germany, 'Application of International Law' (n. 68), p. 5: Finland, 'International law and cyberspace' 2020 (n. 10), p. 3; Iran, 'Declaration' 2020 (n. 106), art. III.

130 ICJ, 'Nicaragua' (n. 89), para. 205; the domaine réservé refers the 'exclusive power to regulate (…) internal affairs', see Jens David Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', *Texas Law Review* 95 (2017), 1579–1598, at 1587.

131 Kunig, 'Prohibition of Intervention' 2008 (n. 123), para. 3: '[G]lobalization leads to an international system of cooperation and interdependence, where more and more problems fall into the sphere of international concern, fewer matters can be regarded as remaining purely domestic. While traditionally the choice and development of a political, economic, social, and cultural system, as well as the formulation of foreign policy remained solely within the domestic jurisdiction, today this sphere has been reduced by numerous international treaties and customary international law'.

enforcement jurisdiction.[132] Restrictions of policy choices e.g. via international law may then be taken into account in a second step. Hence, in line with other commentators this study assumes that the sphere protected by the prohibition of intervention encompasses 'inherently sovereign powers[133]', even if international legal norms on a subject matter exist as well, such as international human rights law.

3. The challenge of asserting coercion in cyberspace

The second constituent element – coercion – is contentious in general, and in cyberspace in particular. No general definition of coercion exists. Under the ICJ dictum a state's decisions must 'remain free ones'.[134] A classical coercive means can be military force but under certain circumstances also economic and diplomatic means may amount to coercive means.[135] At the core of coercion is the element of bending the will of a state[136] or a state adopting a policy that it otherwise would not have taken. Yet, it is inherently challenging to abstractly define the notion of coercion. It is not necessary that a state is the direct target to assume coercion.[137] For example, if a cyber operation targets a private bank of central importance to the financial system of the state it may still be assumed that the state is compelled to change its course of action.

132 Moynihan, 'The Application of International Law' 2019 (n. 58), paras. 106, 107: '[S]tates retain independent authority to make choices among various lawful courses of action on a subject regulated by international law'.

133 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 108; Przemysław Roguski, 'Violations of Territorial Sovereignty in Cyberspace – an Intrusion-Based Approach', in Dennis Broeders/Bibi van den Berg (eds.), *Governing Cyberspace: Behaviour, Power and Diplomacy* (London: Rowman & Littlefield 2020), 65–84, at 79, refers to 'state power' in the context of a potential sovereignty rule.

134 ICJ, 'Nicaragua' (n. 89), para. 205.

135 Christopher C. Joyner, 'Coercion', in in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2006), para. 1.

136 Germany, 'Application of International Law' (n. 68), p. 5: 'Coercion implies that a State's internal processes regarding aspects pertaining to its domaine réservé are significantly influenced or thwarted and that its will is manifestly bent by the foreign State's conduct'.

137 ICJ, 'Nicaragua' (n. 89), para. 205; New Zealand, 'International Law in Cyberspace' 2020 (n. 10), para. 9.

The general challenge of assessing coercion is exacerbated in cyberspace. Cyber operations are usually not characterized by brute physical force but by exploitation of vulnerabilities, deception[138] and often target private entities.[139] Often cyber harm materializes wholly ICT-internal and is not tangible.[140] Furthermore, even for the gravest forms of cyber harm, for example the sabotaging of state-owned critical infrastructure the main harmful effect often already materialize directly from the malicious cyber operation and does not involve exerting pressure on a state. Cyber harm hereby often deviates from straightforward constellations in which the will of a state is bent. Some scholars have hence argued that coercion should not be decisive in cyberspace but rather the question whether an operation prevented a state from freely exercising its functions, potentially even including subconscious influences.[141] Yet, abandoning the coercion requirement may have unwanted repercussions in the broader context of international law. The suggestion has also found little support from states. States have, however, attempted to flexibilize the criteria to varying degrees in cyberspace. Germany suggested that cyber acts equivalent in 'scale and effects' to acts amounting to coercion in non-cyber contexts should be considered coercive when an operation significantly influences or thwarts the will of a state.[142] Australia has referred to the '[effective deprivation](…) of the ability to control, decide upon or govern matters of an inherently sovereign nature'[143], concurring with commentators who argued for the mere '[restriction of] a state's choice with respect to a course of action' as

138 Fischerkeller, 'Current International Law' 2021 (n.125); on coercion via deception and fake news in cyberspace se Björnstjern Baade, 'Fake News and International Law', *European Journal of International Law* 29 (2018), 1357–1376, at 1364.

139 Walton, 'Duties Owed' 2017 (n. 55), 1473: 'Low-intensity cyber attacks struggle to meet this definition because they are typically targeted at private entities, create relatively localized harms within a state, and do not impact policy'.

140 See chapter I.C.I, II.

141 Arguing for abandoning the coercion requirement to protect essential state interests Kilovaty, 'Coercion' 2019 (n. 125), 90.

142 Germany, 'Application of International Law' (n. 68), p. 5: ' Germany is of the opinion that cyber measures may constitute a prohibited intervention under international law if they are comparable in scale and effect to coercion in non-cyber contexts.'

143 Australia's Cyber Engagement Strategy, Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace, 2019, p. 4.

potentially coercive acts.[144] The Netherlands referred to coercion if a cyber operation 'compels' a state to take an action which it otherwise would not pursue'[145], but did not specify under which circumstances 'compelling' can be assumed. It opined that

> '[t]he precise definition of coercion, and thus of unauthorised intervention, has not yet fully crystallised in international law.[146]'

It is difficult to abstractly define criteria such as 'scale and effects' or mere 'restriction of a state's choice'. Furthermore, it is difficult to distinguish undue interferences from certain forms of lesser influence that are usual in international relations.[147] To illustratively assess the merits of states' tendencies to flexibilize coercion in cyberspace the study will in the following analyse specific examples of past cyber operations which have potentially reached the threshold of the prohibition of intervention.

3.1 Interference with elections

Various states, such as Germany[148], Israel[149], the US[150], Ireland[151] or Iran[152], have asserted that interfering with elections via cyber means, e.g. altering election results or manipulating the electoral system or electronic ballots,

144 Sean Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention,' in Jens David Ohlin/Kevin Govern/Claire Finkelstein, *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford: Oxford University Press 2015), 249–270, at 256.

145 Netherlands, 'International Law in Cyberspace' 2019 (n. 15), p. 3.

146 Ibid.

147 Finland, 'International law and cyberspace' 2020 (n. 10), p.3.

148 Germany, 'Application of International Law' (n. 68), p. 5: 'Also, the disabling of election infrastructure and technology such as electronic ballots, etc. by malicious cyber activities may constitute a prohibited intervention, in particular if this compromises or even prevents the holding of an election, or if the results of an election are thereby substantially modified'.

149 Roy Schondorf, Israel Ministry of Justice, Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations, 8 December 2020.

150 Paul C. Ney (2020). DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, Speech of 2 March 2020.

151 Ireland, Position Paper on the Application of International Law in Cyberspace, July 2023, para. 9.

152 Iran, 'Declaration' 2020 (n. 106), Art. III: 'Measures like cyber manipulation of elections or engineering the public opinions on the eve of the elections may be constituted of the examples of gross intervention.'

may violate the prohibition of intervention.[153] Manipulation of electoral data may directly influence who makes governmental decisions and thereby also the content of such choices.

Different from manipulation of electoral processes via technical means is the manipulation of the public discourse via influence operations. Influence operations were particularly prominently discussed during the US presidential elections in 2016 and 2020 regarding alleged Russian interferences. On this matter, states have taken a more ambiguous stance. The question of content harm in cyberspace is outside of the scope of this work[154] but suffice it to note that influence operations regularly face the problem of determining coercion. Single individuals out of the electorate may be influenced but a coercive effect even on a single individual will usually be hard to prove.[155] Furthermore, adopting a broad interpretation of influence operations in the course of elections[156] may risk the legitimization of restrictions on political dissent.

3.2 Intervention in the fundamental operation of parliament

States, such as the UK and Australia, have asserted that cyber operations may be a violation of the prohibition of intervention if they intervene in the 'fundamental operation of parliament'.[157] Neither the UK nor Australia specified under which circumstances they assume that such an intervention takes place. The attacks on Estonia in 2007 and the hack of the German Bundestag in 2015 however are illustrative for deducing criteria for assessing when the fundamental operation of parliament is affected.

153 See also Karine Bannelier/Theodore Christakis, 'Prevention Reactions: The Role of States and Private Actors' (Les Cahiers de la Revue Défense Nationale, Paris, 2017), 44; Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 66, p. 321, para. 25.

154 On the focus on technical cyber harm see chapter 1.B.III.

155 Leonhard Kreuzer, 'Disentangling the Cyber Security Debate', *Völkerrechtsblog*, 20 June 2018, available at: https://voelkerrechtsblog.org/de/disentangling-the-cyber-security-debate/.

156 In a broad interpretation Germany has e.g. hinted at the significant erosion of public trust in a State's political organs and processes as potentially amounting to intervention Germany, 'Application of International Law' (n. 68), p. 5. On the issue of information operations as potential violations of the prohibition of intervention or self-determination Jens David Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', *Texas Law Review* 95 (2017), 1579–1598.

157 UK AG Wright, 'Cyber and International Law' 2018 (n.103); Australia, 'Supplement' 2019 (n.143), p. 2.

The DDoS attack on Estonian institutions in 2007 which lasted for several weeks and inter alia caused the crashing of government websites arguably reached the threshold of intervening in the fundamental operation of parliament. The attacks, likely by so-called 'hacktivists', occurred after the relocation of a statute of a Russian soldier. Unlike mere espionage operations, the DDoS attack caused disruption and significant hampering of governmental services. Furthermore, due to the specific political context the direction of purported influence of the attack was sufficiently clear – the operations occurred to pressure the Estonian legislative and/or executive to either change their prior decision regarding the removal of the statute or to pressure it to take different decisions in the future, hereby aiming to bending its will with regard to a particular policy choice. If such an operation was conducted by a state it would amount to a prohibited intervention. As such an operation hence reached the threshold of significant harm the territorial state from which the operations were predominantly emanating – Russia – was under a due diligence obligation to prevent the attacks.[158]

By contrast, the large-scale cyber espionage operations against the German Bundestag in 2015 for the mere purpose of gaining information lacked a sufficiently clear influential purpose. The operation did not aim to influence a particular political policy decision or to exert pressure. While the EU Council Decision in 2020 based its 'restrictive measures' regarding the Bundestag hack on the argument that the hack 'affected the parliament's information system for several days', and 'affected email accounts'[159], elevating replacement and mitigation efforts to the level of coercion would unduly elevate merely disruptive effects that do not exert pressure to the level of intervention. Replacement of IT may also occur under other circumstances or even be a routine measure, and hence can hardly be said to

158 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 134: 'The attack's severity and sustained nature suggest the application of pressure by another state to deprive Estonia of its free will over the exercise of its sovereign functions. If the cyberattack was designed in order to compel a certain outcome or conduct in Estonia – even if purely to punish or exact retribution – then the activity could meet the threshold of coercive behaviour and thus intervention.'

159 Council of the European Union, Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyberattacks threatening the Union or its Member States, Official Journal of the European Union, L 351 I, Annex: 'This cyber-attack targeted the parliament's information system and affected its operation for several days. A significant amount of data was stolen and the email accounts of several MPs as well as of Chancellor Angela Merkel were affected.'

amount to an intervention with the 'fundamental' operation of parliament. Furthermore, such an extensive interpretation may have ramifications for the interpretation of the norm beyond cyberspace.[160] After all, the EU Council Decision on restrictive measures did not refer to coercion or prohibited intervention.[161] Hence, in this case, the threshold of a prohibited intervention was not met.[162]

To sum up, geopolitical contextual indicators, as well as the mode of operation ('mere' espionage or disruptive DDoS or ransomware operations) may hence be decisive criteria for determining whether an intervention with the 'fundamental operation of parliament' has occurred.

3.3 Cyber operations against critical infrastructure

States have also made clear that they potentially view attacks on critical infrastructure as a violation of the prohibition of intervention. The worthiness of protection of critical infrastructure can be seen in para 13 lit. f, g of the UN GGE Report 2015 which purport a negative obligation of states not to impair critical infrastructure of other states and a duty to protect their own critical infrastructure.[163] Attacks on medical facilities have been highlighted but the term critical infrastructure regularly also includes transport, finance and energy sectors, among others.[164] Also regarding cyber operations against critical infrastructure the question recurs how it is to be determined whether a victim state's will has been bent. For example, the *WannaCry* attack exemplifies that coercion can only be assumed when contextual factors point at a sufficiently clear direction of aimed influence:

160 The damage may be relevant under a potential sovereignty rule, see chapter 3.B.III.5, as well as harm to political institutions as a distinct category of significant harm, see chapter 3.C.IV.3.

161 Referring only to theft of data and interference with parliament's operation without a legal assessment Council, Decision 22 October 2020 (n.159), Annex.

162 Due diligence obligations to prevent may however be triggered in similar constellations if cyber espionage operations against governmental institutions emerge as a distinct category of significant harm, see below chapter 3.C.IV.3.

163 UN GGE Report 2015, para. 13f, g; see in more detail chapter 4.A.I.

164 UK AG Wright, 'Cyber and International Law' 2018 (n. 103): 'Acts like the targeting of essential medical services are no less prohibited interventions, or even armed attacks, when they are committed by cyber means'; highlighting finance, education and social security Costa Rica, Costa Rica's Position on the Application of International Law in Cyberspace, August 2023, para. 25.

The attack e.g. affected UK hospitals, German railway industry, Indian police and hereby interfered with critical infrastructure of several states. Yet, despite its pervasive ramifications on the broader societal level, it is hard to argue that a state was coerced to act in a particular manner. The predominant motivation seemed to be to extort money from victims, or potentially to sow chaos. But due to the lack of further contextual factors and due to the global spread of the attack it is not clear which state actors may have been targeted for the purpose of coercion, regardless of the implications for critical infrastructure.[165]

By contrast, contextual factors existed e.g. in the case of the *Black Energy* or the *Not Petya* attack against Ukraine in 2015 or 2017. Both occurred during the confrontation between Russia and Ukraine, inter alia over the Russian annexation of Crimea. A further case in point is the cyber operation against the Iranian Nuclear Natanz Facility in April 2021, presumably by Israel, which disabled its electricity grid and plausibly aimed at coercing Iran to stop its restarting nuclear enrichment project.[166] When such contextual factors are present an intended coercive effect can be assumed, the threshold of a prohibited intervention is reached and due diligence obligations to prevent (or in the case of the Natanz facility not to cause) significant harm are triggered.

3.4 Impacts on the stability of the financial system

The UK[167] and Australia[168] have argued that also attacks that impact the stability of the financial system may amount to a prohibited intervention. France notably considered that economic harm may even cross the threshold of a use of force.[169] While the choice of an economic system falls within

165 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 140: 'the intention of the perpetrating state in this case appears to have been to extract hard currency from the individual users affected rather than specifically to influence an outcome or conduct in the UK, which was not the original target of the attack'.

166 'Ronen Bergman/Rick Gladstone/Farnaz Fassihi, 'Blackout Hits Iran Nuclear Site in What Appears to Be Israeli Sabotage', *New York Times*, 11 April 2021, available at: https://www.nytimes.com/2021/04/11/world/middleeast/iran-nuclear-natanz.html.

167 UK AG Wright, 'Cyber and International Law' 2018 (n. 103).

168 Australia, 'Supplement' 2019 (n.143), p. 2.

169 France, 'International Law in Cyberspace' 2019 (n.94), p. 8; Finland is also open in this regard Finland, 'International law and cyberspace' 2020 (n. 10), p. 6. Why such

the domaine réservé, integrating economic effects into the prohibition of intervention is tricky and contentious in international law.[170] It must be noted that the financial system depends largely on private actors, such as private banks. It is therefore prima facie difficult to ascertain that the targeting of a single commercial entity may coerce a state.[171] Furthermore, due to the interconnectedness of the international economic order, through trade and finance, mutual economic effects are inevitable. Hence, it is likely that economic effects only exceptionally amount to a prohibited intervention. Arguably, if e.g. a national central bank that has a systemic relevance for the stability of the financial system is targeted by disruptive cyber activities and if subsequently large-scale economic harm occurs that requires a state to intervene and make economic policy choices, a coercive effect can be assumed.[172] It has also been argued that the cyber operations against US financial institutions from 2011 to 2013 by disruptive DDoS attacks amounted to coercion on the US.[173]. As at the time sanctions against Iran – to which the attack was attributed – existed, geopolitical factors make an intended coercive effect on behalf of Iran plausible. However, as several severe cyber operations against financial actors rather resemble vandalism, harm to financial actors or the financial system will only in exceptional cases amount to prohibited intervention. The detrimental consequences of economic harm following cyber operations may also be sufficiently addressed if severe economic harm emerges as a distinct category triggering due diligence obligations.[174] Overzealously elevating economic harm to prohibited intervention seems unnecessary.

---

an extensive interpretation of the use of force in cyberspace is to be rejected see above chapter 3.B.I.2.

170 Kunig, 'Prohibition of Intervention' 2008 (n. 123), para. 25.

171 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 118. 'Thus, if a state-sponsored cyberattack is directed at a single commercial entity such as a private bank (…) this would not engage the state's inherently sovereign functions because it is a private entity rather than a whole sector falling exclusively within the government's powers'.

172 Bobby Vedral, 'The Vulnerability of the Financial System to a Systemic Cyberattack', in in Taťána Jančárková/Lauri Lindström et al. (eds.), *Going Viral* (NATO CCDCOE 2021), 95–110.

173 On the basis that it targeted an entire financial sector Moynihan, 'The Application of International Law' 2019 (n. 58), para. 118.

174 See below chapter 3.C.I.

3.5 Harm to the political and/or cultural system

The choice of a cultural system falls within the domaine réservé. In this vein, France has also broadly referred to 'harm to political and cultural systems' as potential violations of the prohibition of intervention.[175] Open-ended references to cultural systems were also made by Iran[176] or in the joint statement by Russia and China of 2016 which refers to 'disruption of social order, incitement of inter-ethnic, inter-racial and inter-religious antagonism'[177] as potential cyber-induced prohibited interference. While the reference to interference somewhat resonates the *Nicaragua* dictum referring to the choice of 'political and cultural systems', such assertions seem dangerously indeterminate and are likely to be abused without legal specification. As noted in the context of influence operations, extensively interpreting content as harmful may incentivize undue restriction of free speech.[178] Asserting content harm as significant harm triggering due diligence obligations will regularly require close legal scrutiny.

3.6 Undermining the territorial state's exclusive right to enforce the law

In the context of the prohibition of intervention also so-called 'hack-back' operations need to be considered. Via 'hack-back' operations both state and non-state actors on the territory of a third state may aim to disable malicious cyber operations which emanate from another state's territory, e.g. by disabling a server used for an attack.[179] Such hack-back or 'active

175 France, 'International Law in Cyberspace' 2019 (n. 94), p. 7: 'Interference by digital means in the internal or external affairs of France, i.e. interference which causes or may cause harm to France's political, economic, social and cultural system, may constitute a violation of the principle of non-intervention'.

176 Iran, 'Declaration' 2020 (n. 106), Art. III, para. 2: 'Armed intervention and all other forms of intervention or attempt to threaten against the personality of state or political, economic, social, and cultural organs of it through cyber and any other tools are regarded as unlawful.'

177 The Joint Statement Between the Presidents of the People's Republic of China and the Russian Federation on Cooperation in Information Space Development, 26 June 2016, para. 2.

178 See above chapter 3.B.II.2.3.1.

179 In the context of ransomware attacks emanating from Russia US President Biden was asked whether it 'made sense to attack the actual servers that are used in an attack'. He answered in the affirmative, Remarks by President Biden Before Air Force One Departure, 9 July 2021, available at: https://www.whitehouse.gov/briefin

cyber defence'[180] operations can arguably be seen as equivalent to a law enforcement operations. As law enforcement is the exclusive right of a sovereign state and hereby falls into the domaine réservé this raises the question whether such acts reach the threshold of prohibited intervention. The Tallinn Manual rejects that extraterritorial law enforcement violates the prohibition of intervention on the grounds that it is not coercive as an affected state is not 'compelled to act in an involuntary manner or involuntarily refrain from acting in a particular way'.[181] Under the traditional approaches to coercion – e.g. requiring that a state's will is bent or that it is forced to make a policy choice it would otherwise not have taken – extraterritorial law enforcement is indeed hard to grasp as prohibited intervention. If one defines coercion more broadly, e.g. like Australia, as the effective deprivation of the ability to control, decide upon or govern matters of an inherently sovereign nature[182], arguably, hack-back operation by both state or non-state actors would deprive the territorial state of the exclusive right of law enforcement as the territorial state is not able anymore to disable the server itself (or to deliberately choose not to do so). In this reading law enforcement operations, e.g. via so-called hack-back operations, may be considered a violation of the prohibition of intervention. A cyber operation based on Art. 37 of the Swiss Intelligence Law that allows the penetration of servers located abroad to interfere with data in case of attacks against Swiss critical infrastructure[183] would then amount to a prohibited intervention. However, more opinio iuris would be required to determine under which precise conditions extraterritorial enforcement measures by both state and non-state actors reach the threshold of prohibited intervention.[184]

---

g-room/speeches-remarks/2021/07/09/remarks-by-president-biden-before-air-force-one-departure-5/.

180 UK National Cyber Security Strategy 2016–2021, p. 18.

181 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 4, p. 24, para. 22.

182 Australia's Cyber Engagement Strategy, Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace, 2019, p. 4.

183 Switzerland, Bundesnachrichtendienstgesetz 2017, AS 2017 4095, art. 37 (1): 'Werden Computersysteme und Computernetzwerke, die sich im Ausland befinden, für Angriffe auf kritische Infrastrukturen in der Schweiz verwendet, so kann der NDB in diese Computersysteme und Computernetzwerke eindringen, um den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen. Der Bundesrat entscheidet über die Durchführung einer solchen Massnahme (…)'.

184 On extraterritorial enforcement measures as a violation of sovereignty see in the following 3.B.II.2.3.6.

4. Lack of clarity regarding the threshold of prohibited intervention

Overall, the case study reveals a certain degree of uncertainty about the question which cyber operations reach the threshold of prohibited intervention. It is thus no surprise that statements of states on the subject matter persistently call for more clarity on what constitutes an intervention.[185] As with potential violations of the use of force even in cases when a cyber operation arguably violated the prohibition of intervention states have mostly refrained from calling out a violation.[186] Coercion regularly requires contextual factors, such as a geopolitical conflict or indicators regarding the operation's perpetrators. The problem of attributing cyber operations and the ensuing lack of clarity over an attacker's intention however frequently make the assessment of a coercive impact difficult. States are well advised to specify requirements and to highlight particular acts instead of referring to abstract criteria.[187] If a cyber operation reaches the threshold of prohibited intervention the threshold of a risk of significant cyber harm is met, hereby triggering due diligence obligations to prevent.

III. Sovereignty

A further prominent prohibitive rule may be an arguably emerging prohibitive sovereignty rule in cyberspace.

1. The suggestion of a sovereignty rule in cyberspace

The proposition of a sovereignty rule in cyberspace was first put forward by the Tallinn Manual. To address the problem of low-level cyber harm the Tallinn Manual asserted that sovereignty is not only a principle of international law from which distinct primary rules can be derived but a prohibitive primary rule itself:

> 'A State must not conduct cyber operations that violate the sovereignty of another State.'[188]

185 Netherlands, 'International Law in Cyberspace' 2019 (n. 15), p. 3.
186 Efrony/Shany, 'A Rule Book on the Shelf' 2018 (n. 118), 654.
187 See also Germany, 'Application of International Law' 2021 (n. 68), p.6.
188 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), Rule 4.

According to this position, sovereignty hence imposes an obligation on other states not to violate the sovereignty of other states via cyber operations.[189] The suggestion of a sovereignty rule in cyberspace has gained significant momentum among states and scholars.[190] During the last years a significant number of states has opined that sovereignty is a rule of international law applicable in cyberspace, including France[191], the Netherlands[192], Germany[193], Bolivia[194], the Czech Republic[195], New Zealand[196], Japan[197], Iran[198] and the member states of the AU.[199] Other states, such as the US or Israel, have avoided taking a stance[200], potentially employing a 'wait and see' strategy.[201] Only the UK has openly rejected a sovereignty rule in cyberspace.[202] This development suggests that regardless of whether in international law a sovereignty rule exists states have started to embrace such a rule in cyberspace.

189 See the definition of primary Michael Schmitt/Liis Vihul, 'Respect for Sovereignty in Cyberspace', *Texas Law Review* 95 (2017), 1639–1670, Fn. 12: 'Primary rules are those which impose either obligations or prohibitions on States.'

190 See Russell Buchan, *Cyber Espionage and International Law* (Oxford: Hart Publishing 2018), p. 11; François Delerue, 'Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace', in Taťána Jančárková/Lauri Lindström et al. (eds.), *Going Viral* (NATO CCDCOE 2021), 9–24; Kevin Jon Heller, 'In Defense of Pure Sovereignty in Cyberspace', *International Law Studies* 97 (2021), 1432–1499; critical of a sovereignty rule in cyberspace: Gary P. Corn/Robert Taylor, 'Sovereignty in the Age of Cyber', *AJIL Unbound* 111 (2017), 207–212; Oona Hathaway/Alasdair Phillips-Robins, 'COVID-19 and International Law Series: Vaccine Theft, Disinformation, the Law Governing Cyber Operations', *JustSecurity*, 4 December 2020, available at: https://www.justsecurity.org/73699/covid-19-and-international-law-series-vaccine-theft-disinformation-the-law-governing-cyber-operations/.

191 France, 'International Law in Cyberspace' 2019 (n. 94), p. 7.

192 Netherlands, 'International Law in Cyberspace' 2019 (n. 15), p. 2.

193 Germany, 'Application of International Law' 2021 (n. 68), p. 3.

194 OAS, 'Improving Transparency – 4th Report' 2020 (n. 84), para. 52.

195 Czech Republic, Statement by Mr. Richard Kadlčák Special Envoy for Cyberspace Director of Cybersecurity Department in the UN OEWG, 11 February 2020, p. 2, 3.

196 New Zealand, The Application of International Law to State Activity in Cyberspace, 1 December 2020, para. 12.

197 Japan, 'International Law Applicable to Cyber Operations' 2021 (n. 83), p. 2, 3.

198 Iran, 'Declaration' 2020 (n. 106), Art. II, para. 4.

199 AU, 'Common African Position' 2024 (n. 105), para. 13.

200 Schondorf, 'Israel's Perspective' 2020 (n. 149); Ney, 'Remarks Cyber Command' 2020 (n. 150).

201 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 23.

202 UK AG Wright, 'Cyber and International Law' 2018 (n. 103); UK Attorney General Braverman, 'International Law in Future Frontiers', Speech 19 May 2022.

2. Sovereignty as a fundamental principle of international law

The predominant understanding of sovereignty in international law is that sovereignty is a 'pivotal'[203] or fundamental[204] principle of international law from which other international legal norms derive. In the words of the ICJ the 'whole of international law rests [upon it]'.[205] Due to its generality and malleability sovereignty can hardly be defined abstractly in a succinct way. *Crawford* has highlighted that the term is 'susceptible to multiple meanings and rather a catch-all term to the collection of rights held by a state'.[206] Similarly, *Besson* asserted that '[what] sovereignty is (…) [is] determined by the rules of the international legal order'.[207] For example, the prohibition on the use of force and intervention, or jurisdictional rights derive from the principle of sovereignty.[208] Due to this dependency on *distinct* primary rules sovereignty has been described as lacking an intrinsic value[209], an 'opaque notion'[210], or even 'organized hypocrisy'.[211] Under the traditional understanding sovereignty is 'not to be equated with any substantive right'[212] but rather descriptive. It is frequently also invoked in political statements, e.g. for identity claims, without implying legal ramifications.[213] From a legal perspective, 'blunt' or 'sweeping' references to sovereignty are therefore best avoided.[214]

Due to the lack of an intrinsic value or a normative core, the traditional understanding of sovereignty is hence that it is determined by rules of international law but not a primary rule on its own – commentators have

203 Samantha Besson, 'Sovereignty', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2011), para. 1.
204 ICJ, 'Nicaragua' (n. 89), para. 263.
205 Ibid.
206 James Crawford, *Brownlie's Principles of Public International Law* (Oxford: Oxford University Press 2019), 432.
207 Besson, 'Sovereignty' (n.203), para. 109.
208 Netherlands, 'International Law in Cyberspace' 2019 (n. 15), p. 1.
209 Besson, 'Sovereignty' (n.203), para. 109.
210 Heike Krieger, 'Sovereignty – an Empty Vessel?', *EJIL:Talk!*, 7 July 2020, available at: https://www.ejiltalk.org/sovereignty-an-empty-vessel/.
211 Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton: Princeton University Press 1999).
212 Crawford, 'Brownlie's Principles' 2019 (n. 206), 432.
213 Schmitt/Vihul, 'Respect for Sovereignty in Cyberspace' 2017 (n. 189), 1656.
214 Krieger, 'Sovereignty' 2020 (n.210).

called this position the 'sovereignty-as-a-principle-only' approach.[215] This more traditional understanding of sovereignty seems to underlie para. 28 lit. b of the UN GGE Report 2015:

> 'State sovereignty and international norms and principles *that flow from sovereignty* (emphasis added) apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.'[216]

The suggestion of an autonomous sovereignty rule in cyberspace is hence prima facie atypical in international law.

3. 'Violations of sovereignty' in international practice

The editors of the Tallinn Manual and commentators supporting a sovereignty rule have however rightly pointed out that in international legal practice 'violations of sovereignty' have frequently been asserted by states and courts.[217] It is worth taking a closer look at the core of the claims of a violation of sovereignty:

In the *Cosmos 954*[218] and the *ICJ Nuclear Activities*[219] cases violations of sovereignty were based on the occurrence of physical harm. As a specific prohibition on causing significant physical harm exists – the customary obligation not to cause and to prevent significant transboundary harm[220] – the assertions of 'violations of sovereignty' in these cases appear as an argumentative short-cut for referring to interferences with the right to terri-

215 Michael N. Schmitt, 'In Defense of Sovereigtny in Cyberspace', *JustSecurity,* 8 May 2018, available at: https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/.

216 UN GGE Report 2015, para. 28b; UN GGE Report 2021, para. 71 lit. b.

217 Schmitt/Vihul, 'Respect for Sovereignty in Cyberspace' 2017 (n. 189), 1650f.; Luke Chircop, 'Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0', *Melbourne Journal of International Law* 20 (2019), 349–377.

218 *Settlement of Claim Between Canada and the Union of Soviet Socialist Republics for Damage Caused by "Cosmos 954," Canada-U.S.S.R.*, 2 April 1981, para. 17.

219 Application, Nuclear Tests (*Australia v France*), 9 May 1973 ICJ Pleadings 1, para. 3 (ii).

220 ICJ, 'Corfu Channel Case' (n.39), p.22; 'Trail Smelter' (n. 3), 1965; in the reading of this study the harm prevention rule, see chapter 2.B.

torial integrity.[221] It likely would have required more argumentative efforts to assert that the threshold of significant harm was reached or to argue for the customary applicability of the rule in the specific case.

Violations of sovereignty have also been asserted with regard to 'trespassing' cases in which physical incursions into a national airspace or the territorial sea of a state occurred, such as the *Cosmos954* or the *Corfu Channel* cases. In the *Corfu Channel* case the UK had violated Albanian sovereignty by entering the Albanian territorial sea for a minesweeping operation with warships without Albania's consent.[222] In the *Cosmos954* case the Canadian government also argued that, apart from the causation of physical harm, already the trespassing into its airspace constituted a violation of its sovereignty.[223]

Physical incursions into territory can be violations of sovereignty because they affect the territorial integrity of the territorial state. The area-specific rules on incursions by land, air or sea allow for differing levels of incursions. In the law of the sea, rights to access of landlocked countries[224] and rights to innocent passage exist.[225] Also with regard to the regulation of airspace, the content of sovereignty is spelled out in a system of primary rules.[226] While some commentators seem to assume an absolute prohibition against *any* incursion, subject to exceptions[227], the law of the sea example rather suggests that a universal rule regarding physical incursions applying to all areas of the law cannot be presumed.[228]

---

221 In a similar vein, Lahmann describes invocations of sovereignty violations in international practice as mere 'signifier[s] of [a] legally protected interest', not to be confused with the assertion of a prohibitive sovereignty rule, see Henning Christian Lahmann, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace', *Duke Journal of Comparative & International Law* 32 (2021), 61–107, at 95.

222 ICJ, 'Corfu Channel Case' (n.39), p. 36.

223 'Settlement Cosmos954' (n. 218), para. 21.

224 United Nations Convention on the Law of the Sea, 10 December 1982, 1833 UNTS 3, art. 125.

225 Ibid., art. 19; at the time of the *Corfu Channel* case such a right was customarily recognized, see Kari Hakapää, 'Innocent Passage', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2013), para. 2.

226 Chicago Convention on International Civil Aviation, 7 December 1944, 15 UNTS.

227 Heller, 'Pure Sovereignty' 2021 (n. 190), 1458, 1459; Schmitt/Vihul, 'Respect for Sovereignty in Cyberspace' 2017 (n. 189), 1645.

228 See also Gary P. Corn/Robert Taylor, 'Sovereignty in the Age of Cyber', AJIL Unbound 111 (2017), 207–212, at 210; eventually also Schmitt/Vihul do not assume such an absolute prohibition against trespass in cyberspace as they call for identification

Further examples of violations of sovereignty include kidnapping cases – e.g. the abduction of Adolf Eichmann by Israel in Argentina.[229] Abduction both affect the right to territorial integrity and the exclusive right of the territorial state to exercise (enforcement) jurisdiction in its territory.[230]

Remarkably, regarding all these cases it was hence necessary to assess whether rights derived from sovereignty, such as the right to territorial integrity or jurisdictional rights, have been interfered with in order to conclude on a violation of sovereignty. This suggests that sovereignty as such does not stipulate a sufficiently precise prohibitive rule but that the content of sovereignty and correlative prohibitions need to be spelled out in a context-specific manner via reference to primary rules derived from sovereignty but not identical with it.

4. Concepts of sovereignty in cyberspace

Due to the lack of an inherent self-ascertainable content of sovereignty it is the core question whether states have specified the meaning of a potential sovereignty rule in cyberspace. Before turning to suggestions as to the legal content of a sovereignty rule it is necessary to examine how sovereignty in cyberspace has been defined by states conceptually.

Some commentators have noted that it 'depends who you ask what sovereignty in cyberspace is'.[231] Many Western, as well as several American states, merely explain sovereignty in cyberspace as their exclusive right to regulate information and communication technology (ICT) and persons conduct-

of criteria for what constitutes a violation of territorial sovereignty – such identification of criteria would be superfluous if indeed an absolute prohibition against *any* trespass existed, see Schmitt/Vihul, 'Respect for Sovereignty in Cyberspace' 2017 (n. 189), 1647: 'The pressing task is (…) to identify the criteria for violation [of territorial sovereignty] by means of cyber operations'.

229 United Nations, Security Council, Resolution, S/Res/138, 23 June 1960.

230 Stephan Wilske, 'Abduction', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (2019), para. 12; Menno T. Kamminga, 'Extraterritoriality', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2012), para. 23.

231 Mark Pomerleau, ‚What is 'sovereignty' in cyberspace? Depends who you ask', *FifthDomain*, 21 November 2019, available at: https://www.fifthdomain.com/international/2019/11/21/what-is-sovereignty-in-cyberspace-depends-who-you-ask/.

ing cyber activities within their territory.[232] The EU has advanced the concept of European 'technological sovereignty'[233] which does not refer to an overarching legal concept but to a policy concept of strategic autonomy striving to secure European autonomy from foreign technology and service providers in a technical and economic dimension.[234] By contrast, a more elaborate concept of sovereignty in cyberspace was promoted by China in the SCO. A 2011 Draft Code of Conduct asserted 'policy authority for Internet-related public issues' as 'the sovereign right of States'. In particular, it asserted the right to 'protect (…) information space'.[235] As can be seen in lit. c of the Code of Conduct which addresses cooperation to '[curb] dissemination that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment', this information space protection includes inter alia tighter content control in cyberspace.[236] Sovereignty in this regard hence emphasizes the centrality of the state in the regulation of cyberspace, including the regulation of content in cyberspace. In China such control occurs through the so-called 'great firewall'.[237] This conception of sovereignty has implications for the question of internet governance and which level of regulatory control over routing of internet traffic and content

232 OAS, 'Improving Transparency – 4th Report' 2020 (n. 84), para. 51, p. 18; Germany, 'Application of International Law' 2021 (n. 68), p. 3.

233 EU Commission President von der Leyen, 'Shaping Europe's digital future: op-ed by Ursula von der Leyen, President of the European Commission', 19 February 2020; Also the term digital sovereignty is often used, see Tambiama Madiega, 'Digital Sovereignty for Europe', *EPRS – European Parliamentary Research Service*, July 2020.

234 Julia Pohle/Thorsten Thiel, 'Digital sovereignty', *Internet Policy Review* 9 (2020), 1–19, 10.

235 UN General Assembly, International Code of Conduct for Information Security, Annex to the Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, Developments in the field of information and telecommunications in the context of international security, A/66/359, 14 September 2011, lit. e.

236 Reiterating the official stance of the Chinese state Wuhan University/China Institute of Contemporary International Relations/Shanghai Academy of Social Sciences, Sovereignty in Cyberspace: Theory and Practice, p. 3: '[A] state enjoys (…) sovereignty, over cyber infrastructure, entities, behavior as well as relevant data and information in its territory'; Moynihan, 'The Application of International Law' 2019 (n. 58), para. 44.

237 Zhixiong Huang/Kubo Mačák, 'Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches', *Chinese Journal of International Law* 16 (2017), 271–310, at 293.

control, as well as international routes for internet traffic, a state should have.[238]

Definitions of sovereignty in cyberspace hence greatly diverge and have differing consequences regarding Internet governance. When Western states refer to sovereignty in cyberspace, they likely have a very different concept in mind as e.g. countries from the SCO.[239]

5. Legal content of a prohibitive sovereignty rule in cyberspace

Against the background of these divergent concepts of sovereignty in cyberspace suggestions regarding the prohibitive content of a sovereignty rule in cyberspace have been made.

5.1 The absolutist 'pure' sovereigntist approach

The most far-reaching position was taken by France which asserts that any penetration via a digital vector or any production of effects may constitute a violation of sovereignty.[240] Such an absolutist approach to sovereignty, requiring no particular threshold, but potentially already covering mere implant of malware without any loss of functionality as a violation of sovereignty, may be called 'pure sovereigntist'.[241] A number of states have endorsed or taken positions similar to this 'pure sovereigntist' position. Iran e.g. asserted that 'any utilization of cyberspace [which] involves unlawful

238 Danielle Flonk/Markus Jachtenfuchs/Aanke S. Obendiek, 'Authority Conflicts in Internet Governance: Liberals vs. Sovereigntists?', *Global Constitutionalism* 9 (2020), 364–386, at 374; on risks for human rights see Krieger, 'Conceptualizing Cyberwar' 2014 (n. 102), 207.

239 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 170; see also OAS, Improving Transparency': International law and State Cyber Operations (Presented by professor Duncan B. Hollis), 5th Report, CJI/doc. 615/20 rev.1, 7 August 2020, p. 32, para. 45: 'one participant suggested that there may be too many meanings for the term "sovereignty" to ascribe it a rule-like status.'; Henning Christian Lahmann, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace', *Duke Journal of Comparative & International Law* 32 (2021), 61–107, at 91.

240 France, 'International Law in Cyberspace' 2019 (n. 94), p. 6.

241 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 62; Heller, 'Pure Sovereignty' 2021 (n. 190), 1458.

intrusion to the (public or private) cyber structures which is under the control of another state'[242] constitutes a violation of sovereignty. Costa Rica held that espionage operations – and hence 'mere' access operations with no tangible physical consequences – may constitute a violation of sovereignty.[243]Also the AU explicitly rejects a *de minimis* threshold for a violation of sovereignty and takes the position that any unauthorized access constitutes a violation of sovereignty.[244] Switzerland has asserted that 'state sovereignty protects ICT infrastructure on a state's territory against unauthorised intrusion or material damage'[245] which has been interpreted as leaning towards the pure sovereigntist position.[246] Also Guatemala has broadly asserted that taking 'certain information from another State's cyber realm, even when no harm [is caused] that could affect equipment' constitutes a violation of sovereignty.[247] Protests of states against the US National Security Agency (NSA) activities revealed in 2013 have also been interpreted as leaning towards a 'pure sovereigntist' approach[248] but it is not evident that protests against mass-scale surveillance activities can be interpreted as an endorsement of the pure sovereigntist approach which lets even a single penetration suffice. The purist position has also found considerable support among commentators who frequently draw an analogy between the incursion of unauthorized aeroplanes or ships – for which they assume in principle an absolute prohibition – and unauthorized cyber operations.[249]

Yet, two caveats need to be raised: The pure sovereigntist approach is concerning regarding the apparent equation of the exclusive right to territorial sovereignty with a correlative absolute prohibition against *any* form of intrusion. In an interconnected international legal order and in particular in the globally interconnected and decentralized cyberspace such an absolutist concept of sovereignty seems unfit. The idea of a sovereign 'gate' through which any data transfer needs to transit – and the fiction

242 Iran, 'Declaration' 2020 (n. 106), Art. II, para. 4.
243 Costa Rica, Costa Rica's Position on the Application of International Law in Cyberspace, August 2023, para. 22.
244 AU, 'Common African Position' 2024 (n. 105), para. 16.
245 Switzerland, Position Paper on the Application of International Law in Cyberspace, UN GGE 2019/2021, Annex, 2021, p. 2.
246 Heller, 'Pure Sovereignty' 2021 (n. 190), 1459.
247 OAS, 'Improving Transparency – 4th Report' (n. 84), 2020, para. 52.
248 Heller, 'Pure Sovereignty' 2021 (n. 190), 1460.
249 Delerue, 'The Rule of Sovereignty in Cyberspace' 2021 (n. 190), 23; Heller, 'Pure Sovereignty' 2021 (n. 190), 1467; Buchan, 'Cyber Espionage' 2018 (n. 190), 193; Chircop, 'Territorial Sovereignty' 2019 (n. 217), 21.

that a state needs to consent to any 'entry' of data into its territory[250] – would fundamentally challenge the current status of Internet governance in which the ubiquity of non-physical data allows data to seamlessly circulate globally between largely private computer systems.[251]

Furthermore, assuming an analogy between the restrictive regime of airspace control and control over the territorial sea and cyberspace is not convincing. With regard to non-physical transit of data, no border controls occur. For example, there is no water police as in the territorial sea. Unlike the monitoring of a national airspace there is also no central organization that monitors all internet traffic. Only via extensive state control over internet routing and data packaging could such 'trespass' control be approximated. Such an approach, as e.g. enacted by the Russian 'Sovereign Internet Law' from 2019 which enables increased control over data traffic via 'deep packet inspection' measures[252], or the Chinese model requiring assessment of sensitive outbound data[253], essentially contradicts the governance model in particular of Western states and raises several human rights concerns, e.g. regarding freedom of information. Even if proponents of the 'pure' sovereigntist approach do not argue that state are legally entitled to such 'trespass' control, deriving an absolute prohibitive rule against *any* cyber intrusion at least makes claims of the 'sovereigntist' camp plausible that push towards granting states more regulatory control and increased access over routing of internet traffic.[254]

Furthermore, it is telling that the very same states which endorse a pure sovereigntist approach openly resort to offensive operations on the territory of other states. France notably asserts that it would use offensive cyber weapons which aim at 'neutralization of enemy systems' and 'denying

250 Arguably in this direction Russell Buchan, 'Eye on the Spy: International Law, Digital Supply Chains and the SolarWinds and Microsoft Hacks', *Völkerrechtsblog*, 31 March 2021, available at: https://voelkerrechtsblog.org/de/eye-on-the-spy/ 'If this is the case, why does a State's inherently governmental function to decide who enters its sovereign *physical* territory deserve more protection than its decision as to who enters its sovereign *cyber* infrastructure?'.

251 Milton L. Mueller, 'Against Sovereignty in Cyberspace', *International Studies Review* 22 (2020), 779–801, at 789.

252 Acknowledging this legal authority under the Russian law Germany Federal Government, Die menschenrechtlichen Auswirkungen von Social-Media-Zensur und Begrenzungen der Internetfreiheit, BT-Drs. 19/18902, 4 May 2020, p. 6.

253 Mueller, 'Against Sovereignty' 2020 (n. 251), 787.

254 Flonk et al, 'Liberals vs. sovereigntists?' (n. 238), 374.

the availability and confidentiality of adverse systems'.[255] In an apparent contradiction to its pure sovereigntist position it furthermore asserts that espionage as such is not unlawful in international law.[256] The Swiss law on regulation of intelligence operations expressly permits to hack into computer systems located on the territory of another state and potentially alter or delete data if this computer system is used for an attack against the critical infrastructure of Switzerland.[257] The law only requires the authorization of the Swiss government but does not foresee e.g. a prior notification or request for cooperation before the operation begins. While offensive cyber operations may be justifiable under international law, for example as countermeasures or due to necessity[258], it is noteworthy that neither of the states has explicitly conditioned the use of offensive weapons on such justifications. The fact that the very same states endorse offensive cyber operations puts at least a big question mark as to their willingness to adhere to the strict standards of the pure sovereigntist approach they seem to be arguing for. Hence, e.g. *Chircop* who supports a 'pure sovereigntist' approach has acknowledged that this approach cannot 'yet sensibly be described as a crystallised rule of customary international law'.[259]

5.2 Degree of infringement on territorial integrity

An alternative suggestion for the content of a sovereignty rule in cyberspace is the Tallinn Manual's suggestion that a violation of sovereignty may occur depending on the 'degree of infringement on territorial integrity'.[260] Unlike the pure sovereigntist approach which treats any penetration of IT unlawful, this approach focusses on an operation's effects to determine its unlawfulness[261]

255 Déclaration de Mme Florence Parly, Ministre des Armées, sur la stratégie cyber des armées, Paris, 18 January 2019; Arthur P.B. Laudrain, 'France's New Offensive Cyber Doctrine', Lawfareblog, 26 February 2019, available at: https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine.

256 France, 'International Law in Cyberspace' 2019 (n. 94), p. 4, fn. 2.

257 Switzerland, Bundesnachrichtendienstgesetz 2017, AS 2017 4095, art. 37.

258 On the strictly exceptional character of necessity see Lahmann, 'Unilateral Remedies' 2020 (n. 112), 257.

259 Chircop, 'Territorial Sovereignty' 2019 (n. 217), para. 20.

260 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), p. 20, para. 10.

261 On this effects-based approach Roguski, 'Territorial Sovereignty' 2020 (n. 133), 66.

The Tallinn Manual suggests various criteria as indicators for the category of 'degree of infringement upon territorial integrity': Physical damage, loss of functionality of a computer system, and activities below loss of functionality. It assumes that in case one of the first two criteria are fulfilled a violation of sovereignty may have occurred.[262] Regarding the third criterion – activity below loss of functionality, for instance the decelerated performance of a computer, or the alteration or deletion of data without a functional impact, – the Manual remained inconclusive.[263]

Several states have endorsed such an effects-based approach to a sovereignty violation, however without sufficiently specifying their understanding of this largely abstract category. Germany[264], the Czech Republic[265], Finland[266] and Costa Rica[267] have for example endorsed the first criterion proposed by the Tallinn Manual – physical damage. Germany has clarified that also ICT-external physical damage, e.g. resulting from the loss of functionality of ICT may be taken into account for assessing the significance of damage as long as a sufficiently close causal nexus is established.[268] Finland merely referred to 'material harm'.[269] The criteria for assessing the gravity of physical harm hence remain largely unclear. Only the Czech Republic specifically pointed at the 'death or injury to persons' and 'significant physical damage'[270] as violating sovereignty, yet such effects may even amount to a prohibited use of force. Due to the lack of specification it remains unclear which quantitative and qualitative effects physical harm would need to have to amount to a sovereignty violation. It is e.g. unclear which indirect effects would still be counted as sufficiently causally connected physical harm and which degree of physical harm would be considered 'significant'.

The second criterion proposed by the Tallinn Manual has been cautiously endorsed by a few states. Yet, with regard to specification states have so far remained largely inconclusive as well. Germany has e.g. endorsed the second criterion – loss of functionality – and asserted that negligible impairments on their own do not implicate sovereignty as a rule. It how-

262 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 4, p. 20, paras. 11–13.
263 Ibid., para. 14.
264 Germany, 'Application of International Law' 2021 (n. 68), p. 4.
265 Czech Republic, 'Statement UN OEWG' 2020 (n. 195), p. 3.
266 Finland, 'International law and cyberspace' 2020 (n. 10), p. 2.
267 Costa Rica, 'Costa Rica's Position' 2023 (n. 243), para. 20.
268 Germany, 'Application of International Law' 2021 (n. 68), p. 4.
269 Finland, 'International law and cyberspace' 2020 (n. 10), p. 2.
270 Czech Republic, 'Statement UN OEWG' 2020 (n. 195), p. 3.

ever avoided further specification.[271] Similarly, the AU asserted that loss or impairment of functionality of ICT infrastructure may amount to a violation of sovereignty[272] but also fell short of proposing further relevant criteria. Canada and Costa Rica have laudably specified that loss of functionality necessitating the repair or replacement of physical components may amount to a violation of sovereignty[273], while – according to Canada – the mere rebooting or reinstallation of an operating system would likely not suffice.[274] Yet, these specification attempts have so far been isolated and are hence insufficient to discern an emerging opinio iuris.

With regard to the third criterion – activities below loss of functionality – the picture is even more vague. Germany and Finland have highlighted that data modification may be relevant for a potential sovereignty violation but avoided taking a more explicit stance[275], while Ireland has broadly referred to 'interference with data' as a potential sovereignty violation.[276]

Hence, as also the editor of the Tallinn Manual has pointed out[277], more specification is needed to make the degree of infringement criterion operable in practice.

5.3 Interference with or usurpation of inherently governmental functions

The Tallinn Manual suggested a further category of potential sovereignty rule violations: 'Interference or usurpation of inherently governmental

271 Germany, 'Application of International Law' 2021 (n. 68), p. 4.
272 AU, Common African Position 2024 (n. 105), para. 16.
273 Canada, International Law Applicable in Cyberspace, April 2022, paras. 16, 17; Costa Rica, 'Costa Rica's Position' 2023 (n. 243).
274 Canada, International Law Applicable in Cyberspace, April 2022, paras. 16, 17.
275 Ibid.; Finland, 'International law and cyberspace' 2020 (n. 10), p. 2.
276 Ireland, Position Paper on the Application of International Law in Cyberspace, July 2023, para. 6.
277 Michael Schmitt, 'Russia's SolarWinds Operation and International Law', *JustSecurity*, 21 December 2020, available at: https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.

functions'.[278] The suggestion has been endorsed by states, such as the Netherlands[279], the Czech Republic[280], Finland[281], Costa Rica[282] and Guyana.[283]

As with the 'degree of infringement' criterion the content of this criterion is, however, largely unclear. To begin with the first element, it is unclear what an inherently governmental function is. The Tallinn refers to social services, diplomacy, taxes and law enforcement[284] but the notion of inherently governmental functions and in particular its overlap with a state's domaine réservé under the prohibition of intervention remains unclear.[285] Also what amounts to interference or usurpation is not sufficiently specified. The Czech Republic has referred to the s'significant [disruption of] the exercise of those functions, for example distributing ransomware[286]', but it is unclear whether also IT replacement in parliament following espionage operations, e.g. following the *SolarWinds* espionage operation, would amount to an interference.[287] Costa Rica has broadly referred to interferences with elections or health emergency responses as an example for a potential usurpation or interference with inherently governmental functions but it did not specify which technical effects would need to be achieved in order to assume that such an interference has taken place.[288]Tellingly, in the one clear example of a usurpation of inherently governmental functions – extraterritorial law enforcement – states seem to deliberately push the legal assessment towards a grey area. While New Zealand, Costa Rica and the member states of the AU have reiterated extraterritorial law enforcement in cyberspace as a violation of sovereign-

278 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), p. 21, para. 15; the commentaries on the suggestion notably contain hardly *any* reference to state practice or opinio iuris.
279 Netherlands, 'International Law in Cyberspace' 2019 (n. 15), p.3.
280 Czech Republic, 'Statement UN OEWG' 2020 (n. 195), p. 3.
281 Finland, 'International law and cyberspace' 2020 (n. 10), p. 2.
282 Costa Rica, 'Costa Rica's Position' 2023 (n. 243), para. 21.
283 OAS, 'Improving Transparency – 4th Report' 2020 (n. 84), p. 18, para. 52.
284 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 4, p.22, para. 16–18.
285 Ibid., p. 24, para. 22.
286 Czech Republic, 'Statement UN OEWG' 2020 (n. 195), p. 3.
287 Arguing that replacement costs may be the basis for finding a sovereignty rule violation, however based on the 'degree of infringement' criterion Michael N. Schmitt, 'Russia's SolarWinds Operation and International Law', *JustSecurity*, 21 December 2020, available at: https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.
288 Costa Rica, 'Costa Rica's Position' 2023 (n. 243), para. 21.

ty[289] the Netherlands asserted that it is unclear under which circumstances extraterritorial evidence collection without the consent of the territorial state is permitted.[290] Israel has left the question open if extraterritorial law enforcement measures constitute a violation of a potential sovereignty rule, while implicitly acknowledging that such operations take place.[291] Other states which have asserted sovereignty as a primary rule have remained conspicuously mute on the question whether extraterritorial law enforcement constitutes a violation of a sovereignty rule. Already a UN Study on Cybercrime from 2013 suggested that states indeed undertake such direct law enforcement operations which access extraterritorially stored data, even if consensual mutual legal assistance is the more frequent case.[292]

That states are even reluctant to commit to the criterion of extraterritorial law enforcement indicates states' general reluctance to endorse the abstract criterion suggested by the Tallinn Manual. One reason may be that the category of inherently governmental functions, just like the term sovereignty itself, is a highly abstract and politically charged term. States may hence be reluctant to specify their understanding of inherently governmental functions, possibly also due to potential unforeseen ramifications beyond cyberspace. Yet, it also seems emblematic for states' strategic ambiguity[293] to pay lip-service to international law but to conveniently evade legal limitations for own offensive cyber operations.

5.4 Exercise of state power

Close to the pure sovereigntist approach *Roguski* has proposed a nuanced approach by focussing on 'intrusion and interference'.[294] In his view, oper-

289 New Zealand, 'International Law in Cyberspace' 2020 (n. 196), p.2; Costa Rica, 'Costa Rica's Position' 2023 (n. 243), para. 18; AU, 'Common African Position' 2024 (n. 105), para. 15; see also UN Expert Group to Conduct a Comprehensive Study on Cybercrime, Draft Report of 27 July 2020, UNODC/CCPCJ/EG.4/2020/L.1/Add.1, para. 4.

290 Netherlands, 'International Law in Cyberspace' 2019 (n. 15), p. 2.

291 Schondorf, 'Israel's Perspective' 2020 (n. 149).

292 United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, Draft 2013, p. 133.

293 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 23.

294 Roguski, 'Territorial Sovereignty' 2020 (n. 133), 79: '[W]henever a foreign state damages, deletes, deteriorates, alters, or suppresses data stored on a computer system within the territory of another state (…) this action would be regarded as an

ations that affect the integrity of data constitute violations of sovereignty because they resemble the exercise of 'state power'. Operations that 'only' affect the confidentiality of data but not their integrity, such as e.g. phishing operations, would not be considered a violation even if they are conducted with malicious intent.[295] The focus on exercise of state power has the advantage that it mirrors the conceptual definition of sovereignty in cyberspace by Western states. As noted above in particular Western states approach sovereignty in cyberspace predominantly with a view to exclusive jurisdictional rights[296] – and hereby core elements of state power. It partially avoids the rigidity of the absolutist argument against any form of intrusion. Yet, the suggestion is close to the pure sovereigntist approach and hence faces similar concerns to the ones mentioned above. Furthermore, the question remains whether states indeed endorse the position that *any* alteration of data amounts to an exercise of state power.

5.5 Lack of sufficiently clear content of a sovereignty rule in cyberspace

Overall, the prohibitive sovereignty rule endorsed by states in cyberspace lacks a sufficiently specific content to be operable in practice.[297] In this vein, the OAS Report 2020 mentioned the concern that 'there may be too many meanings for the term "sovereignty" to ascribe it a rule-like status'.[298] While the pure sovereigntist approach provides a clear legal content, it may have the effect of plausibilizing claims for tighter state control over cyberspace, with potentially detrimental effects e.g. for freedom of information.[299] Furthermore, states have so far only partially endorsed the abstract effects-based criteria proposed by the Tallinn Manual. Even states that have endorsed the criteria have been reluctant to further specify and commit to more specific criteria.

---

exercise of state power and thus a violation of the territorial sovereignty of the targeted state.'

295 Ibid.

296 See above chapter 3.B.III.4.

297 See also Barrie Sander, 'Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections', *Chinese Journal of International Law* 18 (2019), 1–56, at 19–20.

298 OAS, 'Improving Transparency – 5th Report' 2020 (n. 239), p. 32, para. 45.

299 Leonhard Kreuzer, 'Sovereignty in Cyberspace – A Rule Without Content?, in Antonio Segura Serrano (ed.), *Global Cybersecurity and International Law* (London: Routledge 2024), 29–43, at 43.

Considering the wide endorsement of a sovereignty rule in cyberspace this result is baffling, yet is emblematic for states' Janus-faced approach to international law: On the one hand, states invoke international law, inter alia for deterrent purposes. On the other hand, they strategically avoid to commit to sufficiently precise rules for their own offensive cyber operations. Due to the potentially complex ramifications of committing to a precise legal content of a sovereignty rule it seems doubtful whether states are more willing to come forward with regard to the specification of a sovereignty rule in cyberspace in the future.

6. Assessing risks and benefits of a sovereignty rule in cyberspace

This result raises doubts about the potential and desirability of a prohibitive sovereignty rule in cyberspace. Commentators frequently assert that a central benefit of a sovereignty rule is that it may provide for the basis for taking countermeasures.[300] The lack of a sufficiently clear content of a sovereignty rule, however, directly challenges this assumption as it seems unlikely that states will invoke violations of sovereignty to justify countermeasures. The practical utility of a sovereignty rule in cyberspace as a basis for countermeasures may be questioned in two further respects: First, a sovereignty rule would still need to overcome the attribution problem.[301] In cyberspace, legal – as opposed to political – attribution is notoriously problematic.[302] Even if a malicious cyber operation is de facto state-sponsored, it is challenging to legally prove it with sufficient certainty in a

300 Schmitt/Vihul, 'Respect for Sovereignty in Cyberspace' 2017 (n. 189), 1669.

301 Acknowledging the persisting attribution problem Heller, 'Pure Sovereignty' 2021 (n. 190), 1437; highlighting that attribution is still necessary to conclude on the violation of a prohibitive sovereignty rule AU, 'Common African Position' 2024 (n. 105), para. 19.

302 On political attribution see Netherlands, 'International Law in Cyberspace' 2019 (n. 15), p. 6: '[political attribution is] a policy consideration whereby the decision is made to attribute (publicly or otherwise) a specific cyber operation to an actor without necessarily attaching legal consequences to the decision (such as taking countermeasures).' On the problems of attribution generally Lahmann, 'Unilateral Remedies' 2020 (n. 112), 109, 110; Nicholas Tsagourias/Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges', *European Journal of International Law* 31 (2020), 941–967; see also Introduction.

timely manner.[303] Furthermore, states are generally reluctant to resort to countermeasures following a cyber operation.[304] States hence lean towards a strategic sidelining of the legal regime of countermeasures, as exemplarily expressed by a US official following ransomware attacks, presumably originating from Russia, in July 2021:

> 'We're not going to telegraph what those [re]actions will be, precisely. Some will be manifest and visible, some of them may not be, but we expect those to take place in the days and weeks ahead.'

The indeterminacy of a sovereignty rule brings the risk that it is (mis)used as a highly discretionary norm for resorting to countermeasures in cases when sufficient legal criteria lack. If indeed any cyber intrusion constituted a violation of a sovereignty rule, then in principle any hacking operation would need to be considered a potential violation of sovereignty (until it is determined that non-state actors are responsible and the operation is not attributable). Such a presumed state of persistent norm violation[305] may trigger an escalatory spiral which international law is designed to prevent.

As a further downside, a sovereignty rule may embolden authoritarian and sovereigntist approaches to state control over cyberspace. It is likely that more authoritarian states will invoke a broad understanding of sovereignty[306], in particular with regard to content such states perceive as harmful.[307] The lack of clarity of what sovereignty in cyberspace entails may give authoritarian states a blueprint to invoke the concept for purposes

303 The fact that a cyber operation was launched from the territory of a state is insufficient to attribute the operation to that state, see e.g.UN GGE Report 2021, para. 71g: '[T]he Group recalls that the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State; and notes that accusations of organizing and implementing wrongful acts brought against States should be substantiated'.

304 Efrony/Shany, 'A Rule Book on the Shelf' 2018 (n. 118), 654.

305 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 61.

306 Highlighting this risk Ireland, 'Application of International Law in Cyberspace' 2023 (n. 276), para. 7; see also Moynihan, 'The Application of International Law' 2019 (n. 58), para. 62; Lahmann, 'Politics and Ideologies' 2021 (n. 239), 91.

307 Oona Hathaway/Alasdair Phillips-Robins, 'COVID-19 and International Law Series: Vaccine Theft, Disinformation, the Law Governing Cyber Operations', *JustSecurity*, 4 December 2020, available at: https://www.justsecurity.org/73699/covid-19-and-international-law-series-vaccine-theft-disinformation-the-law-governing-cyber-operations/.

undermining human rights. A sovereignty rule may hereby prove a Trojan horse for Western states, also in areas beyond cyberspace.

Therefore, overall, better arguments speak against a sovereignty rule in cyberspace. If states would, however, move towards specifying a sovereignty rule in cyberspace with sufficient clarity cyber operations that would reach the threshold of such a prohibitive norm would trigger due diligence obligations to prevent.

C. Significant cyber harm beyond acts reaching the threshold of prohibitive rules

Beyond cyber harm reaching the threshold of prohibitive international legal rules also the risk of 'mere' significant harm triggers due diligence obligations to prevent. While the notion of significant harm carries an inherent ambiguity this can also be considered a strength[308] as an aptly flexible criterion for the technologically new area of cyberspace. The broad benchmark for the significance of a risk of harm is whether it has become a 'concern in inter-state relations'[309], and by considering quantitative and qualitative criteria for assessing the degree of cyber harm.

I. Economic cyber harm as a category of significant cyber harm

One category of cyber harm that may be considered an emerging category of significant harm is economic harm. The harm prevention rule is open to include also economic damages as relevant harm. Although the ILC excluded non-physical harm from its Draft Articles on Prevention[310], Art. 2 acknowledges that harm to property can also be relevant harm.[311] That the

308 Crootof, 'International Cybertorts' 2018 (n. 9), 608: 'Indeed, as is often the case in international technological regulation, the inherent ambiguity of "significant harm" is a strength: it is a relatively tech-neutral standard that permits coherent but flexible legal development.'

309 Schmitt, 'In Defense of Due Diligence' 2015 (n. 54), 76.

310 To keep the principles more manageable, see Bäumler, 'Schädigungsverbot' 2017 (n. 2), 64f.

311 ILC Draft Articles on Prevention (n. 6), art. 2b: '"Harm" means harm caused to persons, property or the environment.'

harm prevention rule can address economic harm is also evidenced by its relevance in international finance law and international trade law.[312]

1. The problem of economic cyber harm

Economic harm can occur through a variety of malicious cyber activities. Cyber espionage can lead to theft of intellectual property or trade secrets. The manipulation of financial, corporate or customer data may have severe economic consequences for businesses and individuals, and e.g. lead to lost productivity or reputational harm.[313] Also replacement costs of infiltrated IT systems and necessary financial efforts for more cyber resilience, e.g. cyber insurance, can be considered sufficiently causally connected consequences of cyber harm.[314] In recent years the threat of ransomware attacks against businesses, which encrypt data and demand a ransom for its decryption, has increased. In July 2021, for example, about 400 supermarkets in Sweden had to close due to ransomware attacks that affected its payment and check out system.[315] While statistical assessments diverge, the threat of economic cyber harm is unanimously tremendous: Estimates range from 1 trillion[316] to 10,5 trillion USD damage annually by 2025[317] – which would

312 Bäumler, 'Schädigungsverbot' 2017 (n. 2), 122; Krajewski, 'Due Diligence in International Trade Law' 2020 (n. 66), 312–328. Beyond the harm prevention rule stipulating binding due diligence obligations also *soft law* diligence requirements for 'doing' due diligence exist in international economic law, see e.g. in international tax law; on voluntary 'doing' due diligence standards (as opposed to binding due diligence obligations) see chapter 2.B.

313 Christian Calliess/Ansgar Baumgarten, 'Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective', *German Law Journal* 21 (2020),1149–1179, at 1151.

314 McAfee, 'Economic Impact of Cybercrime— No Slowing Down', February 2018, p. 6.

315 Joe Tidy, 'Swedish Coop supermarkets shut due to US ransomware cyber-attack', *BBCNews*, 3 July 2021, available at: https://www.bbc.com/news/technology-57707530.

316 Zhanna Malekos Smith/Eugenia Lostri/James A. Lewis (Project Director), McAfee, 'The Hidden Costs of Cybercrime', 9 December 2020, p. 3.

317 Steve Morgan, 'Cybercrime To Cost The World $10.5 Trillion Annually By 2025', 13 November 2020, available at: https://cybersecurityventures.com/annual-cybercrime-report-2020/; Prableen Bajpai, 'The 5 Largest Economies In The World And Their Growth In 2020', *Nasdaq*, 22 January 2020, available at: https://www.nasdaq.com/articles/the-5-largest-economies-in-the-world-and-their-growth-in-2020-2020-01-22.

make the economic damage from cybercrime the third largest economy after the US and China if it was a country.[318] Due to the expanding attack surface that comes along with the continuously increasing social interconnectivity the economic damage from cyber harm is expected to continue to rise in the near future.[319]

2. Increasing concern about economic cyber harm

It hence comes as no surprise that states are heavily concerned about economic and financial harm caused by malicious cyber activities. The UN GGE and the UN OEWG Reports emphasized the concern about economic harm from malicious cyber activities[320] and also the Tallinn Manual acknowledged the increasing concern about economic cyber harm.[321] Also, states have made clear in protests or reactions that they consider certain forms of economic harm inacceptable in international relations. For example, the first EU Council Decision on 'restrictive measures against cyber attacks' in July 2020 was inter alia based on the fact that 'significant economic loss' had occurred.[322] The US considered the economic harm inflicted on Sony in 2014, presumably by North Korea, as 'outside the bonds of acceptable state behaviour'.[323] With regard to the persistent DDoS attacks

318 Bajpai, 'Largest Economies' 2020 (n. 318).

319 Morgan, 'Cybercrime Cost' 2020 (n. 318).

320 UN OEWG, Final Report 2021, paras. 18, 19; 'States concluded that there are potentially devastating security, economic (…) consequences of malicious ICT activities on critical infrastructure (CI) and critical information infrastructure (CII) (…) States also concluded that ICT activity contrary to obligations under international law (…) could pose a threat […to] economic development and livelihoods (…)'; UN GGE Report 2021, para. 8; UN GGE Report 2015, para. 7.

321 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 4, para. 28, 'The International Group of Experts acknowledged that States appear to be increasingly concerned about cyber operations that result in severe economic loss (…)'.

322 Council of the European Union, Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, L 246/12, Annex:'Operation Cloud Hopper" targeted information systems of multinational companies in six continents, (…) resulting in significant economic loss; (…) NotPetya" or "EternalPetya" rendered data inaccessible (…) resulting amongst others in significant economic loss.'

323 US, Federal Bureau of Investigation, Update on Sony Investigation, 19 December 2014.

on US financial institutions in 2016 the US indicted seven Iranian hackers, basing its indictment inter alia on the high remediation costs required and that the attacks sabotaged US financial institutions and undermined the integrity of fair competition.[324] France considered economic cyber harm even as a potential use of force.[325] Such a rather far-fetched interpretation would likely lead to a risk of escalation, in particular in areas outside of cyberspace. But it similarly exemplifies that the concern about economic cyber harm is pervasive.

3. Criteria for assessing the significance of economic harm

As it is clear that not every economic harm caused by cyber activities triggers due diligence duties to prevent, criteria are necessary for assessing when economic harm crosses the threshold of significance and hereby triggers due diligence duties. The difficulty of assessing economic harm makes the determination of a precise threshold of prohibited economic harm particularly complex.[326] Yet, assessing different degrees of economic harm in international law is not *per se* unfeasible. For example, in international trade law tribunals have contributed to specifying criteria for assessing the gravity of economic harm.[327]

3.1 Violation of intellectual property rights and trade secrets

An important category of significant economic cyber harm may be the degree of interference with intellectual property rights and trade secrets, and consequent harmful effects, e.g. on fair competition. Other harmful

324 US Department of Justice, 'Manhattan U.S. Attorney Announces Charges against Seven Iranians for Conducting Coordinated Campaign of Cyber Attacks against U.S. Financial Sector on Behalf of Islamic Revolutionary Guard Corps-Sponsored Entities', Press Release 24 Mach 2016.

325 France, 'International Law in Cyberspace' 2019 (n. 94), p. 8.

326 This difficulty is also reflected in the contested discussions around economic pressure or coercion as a use of force or a prohibited intervention, on this issue see Kunig, 'Prohibition of Intervention' 2008 (n. 123), para. 25.

327 Bäumler, 'Schädigungsverbot' 2017 (n. 2), 122f.

consequences may be, inter alia, the hampering of 'research, trial, manufacture, and distribution of vaccines'[328] in the health sector.

States have repeatedly pushed back against intellectual property violations via cyber means of both state and non-state actors. The EU Cyber sanction decision regarding '*Operation Ground Hopper*' and '*NotPetya*' was e.g. inter alia based on infringement of intellectual property rights, stating as a reason for the restrictive measure that 'commercially sensitive data [had been accessed without authorization]'[329], hereby reflecting Art. 3 lit. d of the EU Cyber Decision which lists theft of intellectual property as a relevant factor for determining whether a significant effect constitutes an external threat to the Union or its member states.[330] The US and the UK have protested against infringements of intellectual property on vaccine research during the COVID-pandemic[331] and also Switzerland and Germany have made clear that they consider economically motivated espionage as harmful.[332] Also, international legal scholars have highlighted the relevance of 'significant costs of targeted facilities' as relevant harm following espionage operations against intellectual property.[333]

States have furthermore aimed at reducing intellectual property violations through non-binding informal agreements. Such informal agreements and statements reflect both the positive preventive, as well as the negative prohibitive dimension. Regarding the positive preventive dimension the Western-led Paris Call for Trust and Security of 2018 e.g. called on states to prevent theft of intellectual property.[334] Reflecting the prohibitive negative

328 See ELAC, 'Oxford Statement Health Care Sector' 2020 (n. 18).

329 Council of the European Union, Decision 2020/1127 (n. 322), Annex.

330 Council of the European Union, Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 7299/19, 14 May 2019, art. 3d: 'The factors determining whether a cyber-attack has a significant effect as referred to in Article 1(1) include (…) the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property.'

331 UK, Foreign Secretary, 'UK condemns Russian Intelligence Services over vaccine cyber attacks', 16 July 2020.

332 On this stance Homburger, 'Recommendation 13a' 2017 (n. 54), para. 19; Switzerland, Submission of Switzerland to the United Nations Secretary-General's report, (A/72/315).

333 See ELAC, 'Oxford Statement Health Care Sector' 2020 (n. 18), para. 2: 'International law prohibits cyber operations by States that have significant adverse or harmful consequences for the research, trial, manufacture, and distribution of a COVID-19 vaccine, including by means (…) which impose significant costs on targeted facilities in the form of repair, shutdown, or related preventive activities'.

334 Paris Call 2018 (n. 11), p.3.

dimension of the harm prevention rule, ASEAN and the US declared in a statement that no state should 'conduct or knowingly support ICT-enabled theft of IP'[335], reiterating a similar declaration made in the MoU of 2015 between the US and China, and UK and China.[336]

A G20 statement e.g. linked protection of intellectual property to responsible state behavior (which in principle includes the harm prevention rule and its diligence aspects).[337] Additionally, several commentators have highlighted that harm to intellectual property may be considered significant harm under the harm prevention rule.[338] These developments indicate that cyber harm against intellectual property may amount to significant harm that triggers due diligence obligations to prevent.[339]

Grasping cyber harm to intellectual property as relevant harm under the harm prevention rule has an important gap-filling function: While the right to intellectual property is protected by the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) of the World Trade Organization (WTO), in particular by Art. 39 TRIPS this protection is limited. Art. 39 (1), (3) TRIPS requires states to protect undisclosed information

335 ASEAN – US Cybersecurity Cooperation, Statement, 15 November 2018: '(…) [N]o State should conduct or knowingly support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors (…)'.

336 U.S.-China Cyber Agreement, 16 October 2015, 'the United States and China agreed (…) refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property'; UK Foreign & Commonwealth Office, 'UK-China Joint Statement 2015', 22 October 2015, https://www.gov.uk/government/news/uk-china-joint-statement-2015: 'The UK and China agree not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of providing competitive advantage'; Moynihan, 'The Application of International Law' 2019 (n. 58), para. 145.

337 G20 Leaders' Communiqué, 16 November 2015, para. 26: '(…) we affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors (…) we (…) commit ourselves to the view that all states should abide by norms of responsible state behaviour in the use of ICTs'.

338 Arguing for state accountability for economic espionage based on the ICJ *Corfu Channel* rationale Christina Parajon Skinner, 'An International Law Response to Economic Cyber Espionage', *Connecticut Law Review* 46 (2014) 1165–1207, at 1192; Antonio Coco/Talita de Souza Dias/Tsvetelina van Benthem, 'Illegal: The SolarWinds Hack under International Law', *European Journal of International Law* 33 (2022), 1275–1286, at 1283.

339 In this vein Coco/Dias/van Benthem, '*The SolarWinds Hack*' 2022 (n. 338), 1283.

or data in order to prevent unfair competition.[340] The predominant understanding of Art. 39 TRIPS is however that its protective scope is limited to a state's territory.[341] Hence, in this reading, Art. 39 TRIPS neither entails a prohibition to conduct economic espionage on the territory of a third state, nor an obligation to prevent such activities emanating from a state's territory. Integrating economic cyber harm to intellectual property within the scope of the harm prevention rule would fill this gap.

The big question is whether any infiltration of intellectual property and trade secrets on another state's territory via cyber means is considered significant harm. The protests against espionage against single vaccine centres, e.g. by the UK and the US, shows that in principle also operations against a single entity may amount to a concern in inter-state relations. Yet, if any compromising of intellectual property sufficed, this would, as a consequence, lead to an extraterritorial extension of the protective scope of Art. 39 TRIPS via the harm prevention rule. As the TRIPS agreement may be considered *lex specialis* it seems more convincing to assume that the protective scope under the customary harm prevention rule is lower and that not every risk of a violation of intellectual property triggers due diligence duties to prevent. A possible approach could hence be that harmful effects of a substantial number of cyber espionage operations cumulatively amount

340 WTO, Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), 15 April 1994, Annex 1C, Marrakesh Agreement Establishing the World Trade Organization, 1869 UNTS 299, 33 ILM 1197 (1994), art. 39 (1), (3): 'In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 3. (…) In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use.' All 164 WTO member states are party to the TRIPS agreement. Protection against unfair competition was already granted by Article 10bis which prohibits acts that constitute unfair competition, Paris Convention (incorporated into TRIPS), art. 10bis.

341 David P. Fidler, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies', *ASIL Insights*, 20 March 2013, available at: www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-internationallaw-controversies-involving; Jamie Strawbridge, 'The Big Bluff: Obama, Cyber Economic Espionage, and the Threat of WTO Litigation', *Georgetown Journal of International Law* 47 (2016), 833–870; but arguing for the extraterritorial application of Art. 39.2 TRIPS and Art. 10bis Paris Convention as prohibiting economic espionage Buchan, 'Cyber Espionage' 2018 (n. 190), 133, 141.

to significant harm. Eventually, states need to be more forthcoming in their opinio iuris to clarify the threshold.

3.2 Further criteria for assessing the gravity of economic harm

In which further constellations disruptive and destructive cyber harm amounts to significant economic harm is difficult to determine. For example, under which circumstances does a ransomware operation against a business or individual constitute significant harm? State practice, opinio iuris and international legal documents provide some, yet so far ambiguous hints.

With regard to ransomware, US president Biden broadly asserted that:

> '[The] United States expects when a ransomware operation is coming from [Russia's] soil – even though it's not sponsored by the state – we expect [Russia] to act. And we've given [Russia] enough information to act on who that is'[342]

hereby suggesting that in principle any ransomware operation triggers due diligence duties to prevent harm. Yet, such an approach seems so far to be an outlier. Taking a quantitative approach, Art. 3 lit. d of the EU Council Cyber Sanctions Decision of May 2019 concerning 'restrictive measures against cyber-attacks threatening the Union or its Member States' determines the 'amount of economic loss' as a relevant factor for determining the question whether a cyber attack has a 'significant effect'.[343] More open-endedly, Art. 3 lit. a lists the 'disruption of economic activities' as a relevant criterion for the determination of malicious cyber activities with a 'significant effect'[344] and specifies the 'scope, scale, impact or severity'[345]

342 CNN, 'Biden warns Putin during call that 'we expect him to act' on Russian ransomware attacks', *CNN* 9 July 2021, available at: https://edition.cnn.com/2021/07/09/politics/biden-putin-call-syria-ransomware/index.html.

343 Council of the European Union, Decision 7299/19 2019 (n.330), art. 3: 'The factors determining whether a cyber-attack has a significant effect as referred to in Article 1(1) include (…) (d) the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property'.

344 Ibid., art. 3a. The classification of a significant effect 'only' triggers the applicability of restrictive measures – as retorsion – and hence is not tantamount to a categorization as internationally wrongful. It nevertheless indicates legal criteria based on which states will respond to a malicious operation.

345 Council of the European Union, Decision 7299/19 2019 (n. 330), art. 3a.

and the 'numbers of persons affected' as criteria for assessing whether a cyber operations has a significant effect.[346] Similarly open-endedly the Czech Republic considered a significant impact on its economy as a relevant factor for the question if an act amounts to a violation of international law.[347] The now-repealed EU Directive on the security of network and information system (NIS) 2016/1148 stipulated the market share of an entity and the geographical scope of its economic operations as criteria to determine when cyber operations have significant disruptive effects on the provision of critical services.[348] While these criteria concerned disruptive effects on critical infrastructure they seem equally useful for the general assessment of the significance of economic harm.

None of the above-mentioned criteria have been sufficiently endorsed by states to be considered *lex lata* and hence so far have only exemplary character. As a bottomline, however, the various examples of open-ended sliding-scale criteria weigh against assuming significant economic cyber harm already at a very low-level, e.g. with regard to a single ransomware operation. However, it should be recalled that also many minor harmful acts which on their own do not reach the significance threshold may cumulatively be considered significant harm, as the *Trail Smelter* case shows.[349]

4. Economic harm as an emerging category of significant cyber harm

Economic cyber harm is a strong candidate for significant harm under the harm prevention rule. Due to the manifold economic ramifications of cyber operations and insufficient opinio iuris it is however difficult to comprehensively assess which economic cyber harm is most relevant. It is clear that states are particularly concerned about theft of intellectual property and trade secrets via economic cyber espionage. However, it is so far unclear if *any* theft of intellectual property or trade secrets is considered

346 Ibid., art. 3b.

347 In the context of a potential sovereignty Czech Republic, 'Statement UN OEWG' 2020 (n. 195), p. 3.

348 Directive (EU) 2016/1148, 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union, art. 6 lit. d, e. The directive uses the term essential service but this is largely equivalent to critical infrastructure, see the similarity of the definition of essential service, art. 5 (2), to the understanding of critical infrastructure in the international legal discourse, below chapter 3.C.II.3.

349 See above chapter 3.A.V.

significant, hereby triggering due diligence obligations to prevent. States are well advised to specify their opinio iuris in this regard. The same applies to the more ambiguous question which degree of economic harm beyond access operations amounts to significant harm, e.g. under which circumstances ransomware operations amount to significant harm. A variety of potential quantitative and qualitative criteria exist, yet states have not yet sufficiently endorsed them.

II. Cyber harm to critical infrastructure as a category of significant cyber harm

A further category of significant cyber harm may be cyber harm to critical infrastructure. Malicious cyber operations against critical infrastructure are a grave threat for both national and international security. In December 2015 the attack with *Black energy* malware caused power outage for six hours to hundreds of thousands of homes in the Ukraine.[350] In the US, ransomware paralyzed a hydroelectric power plant.[351] Malicious cyber operations against hospitals during the COVID-pandemic with ransomware disabled the delivery of medical services during an acutely vulnerable period.[352] In May 2020, an Iranian port was targeted by malicious cyber operations for several days, its operation was disrupted, causing traffic jams and delays in shipment.[353] In September 2020, a cyber operation against a German hospital caused delayed treatment of a woman who had to be

350 Kim Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', *Wired,* 3 March 2016, available at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

351 Jan Kleijssen/Pierluigi Perri, 'Cybercrime, Evidence and Territoriality: Issues and Options', in Martin Kuijer/Wouter Werner (eds.), *The Changing Nature of Territoriality in International Law* (Netherlands Yearbook of International Law 2016), 147–173, at 153.

352 See the condemnation by Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic, 30 April 2020: 'Since the beginning of the pandemic, significant phishing and malware distribution campaigns, scanning activities and distributed denial-of-service (DDoS) attacks have been detected, some affecting critical infrastructures that are essential to managing this crisis (…) Any attempt to hamper the ability of critical infrastructures is unacceptable.'

353 Ronen Bergman/David M Halbfinger, 'Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks', *New York Times*, 18 May 2021, available at: https://www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyberattacks.html.

transferred to another hospital and subsequently died.[354] The list of cyber operations against critical infrastructure could be extended substantially, yet the list of attempted attacks is even longer. For example, in April 2020, hackers unsuccessfully tried to penetrate the SCADA of wind turbines in Azerbaijan; in another case, hackers unsuccessfully tried to penetrate the command and control system of water treatment plants, pumping stations and sewages in Israel.[355] There are further instances in which potentially devastating consequences of malicious cyber operations could be averted. It is hence evident that malicious cyber operations against critical infrastructure can have the gravest consequences for nation states, society and individuals.[356]

1. Increasing concern about cyber operations against critical infrastructure

The concern about cyber harm to critical infrastructure is a 'cross-cutting theme' in UN resolutions since the turn of the millennium.[357] The UN GGE Report of 2015 stated:

> 'The most harmful attacks using ICTs include those targeted against the critical infrastructure and associated information systems of a State. The risk of harmful ICT attacks against critical infrastructure is both real and serious.'[358]

354 Although it is not clear whether the death could have been avoided without the delayed treatment Melissa Eddy/Nicole Pelroth, 'Cyber Attack Suspected in German Woman's Death', *New York Times*, 18 September 2020, available at: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.

355 For a continuously updated list of international cyber incidents, including the two mentioned here see https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

356 Eric Talbot Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense' *Stanford Journal of International Law* 38 (2002), 207–240, at 207.

357 Michael Berk, 'Recommendations 13 (g) and (h)', in Eneken Tikk (ed.) *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary,* (United Nations Office for Disarmament Affairs 2017), 191–222, at 197, 198, paras. 14, 15.

358 UN GGE Report 2015, para. 5.

The UN OEWG Final Report highlighted the potentially 'devastating consequences' of malicious cyber operations against critical infrastructure.[359] Also the UN GGE Report 2021 noted the increasingly serious character of malicious cyber operations against critical infrastructure.[360] Therefore, it is clear that malicious cyber operations against critical infrastructure have become a core concern of states in international law.

2. Diverging definitions of critical infrastructure

The commentaries to the Budapest Convention provide a widely agreeable bottomline of what critical infrastructure is. According to this commentary critical infrastructure

> 'can be defined as systems and assets, whether physical or virtual, so vital to a country that their improper functioning, incapacity or destruction would have a debilitating impact on national security and defence, economic security, public health or safety, or any combination of those matters.'[361]

States' precise definitions of critical infrastructure however diverge. Some are extremely wide, like the one by Russia which would potentially include any governmental agency as critical infrastructure.[362] The definition of the

359 UN OEWG Final Report 2021, para. 18: 'States concluded that there are potentially devastating security, economic, social and humanitarian consequences of malicious ICT activities on critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public.'

360 UN GGE Report 2021, para. 10: 'Harmful ICT activity against critical infrastructure that provides services domestically, regionally or globally, which was discussed in earlier GGE reports, has become increasingly serious.'

361 Cybercrime Convention Committee (T-CY), T-CY Guidance Notes, T-CY (2013)29, 8 October 2013, p. 15; the Tallinn Manual gives a similar definition, Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), Glossary, p. 564: 'Physical or virtual systems and assets of a State that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment.'

362 Russia, Federal Law of the Russian Federation, 26 July 2017, No. 187-FZ, art. 2: 'Critical infrastructure facilities" shall mean facilities, systems and institutions of the state which conduct their activities in the interests of the state, national defense or security, including individual security'.

US also includes commercial facilities[363], while the definition of Uruguay includes 'any service that affects more than 30 % of the population'.[364]

Despite all deviations it is notable that almost all definitions list a number of key critical infrastructures: These are medical services, financial services, governmental services, food, transportation, communication, energy and water supply.[365]

Beyond these key critical infrastructures states deviate in their designation of sectors and entities as critical infrastructure. It is for example unclear whether electoral processes are considered critical infrastructure.[366] Considering that globally a significant number of states are not democratic and that furthermore also democratic states like the US have only added electoral infrastructure to the list of critical infrastructure in January 2017[367] this tentatively weighs against assessing electoral processes as critical infrastructure. Furthermore, interference with electoral processes may violate the prohibition of intervention.[368] Consequently, strengthening their protection by categorizing it as critical infrastructure does not seem necessary in order to grant them due protection under international law.

363 US, White House, 'Critical Infrastructure Security and Resilience' (2013) Presidential Policy Directive/PPD-21.

364 Uruguay, Comments on the pre-draft of the UN OEWG report, p. 3, para. 5.

365 Delerue, 'Cyber Operations' 2020 (n. 107), 298; ITU, Guide to Developing a National Cybersecurity Strategy, 2018, p. 42; see e.g. Australia Department of Home Affairs, Critical infrastructure resilience, names banking and finance, government, communications, energy, food and grocery, health, transport, water as critical infrastructure, available at: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/critical-infrastructure-resilience.

366 In favour e.g. Netherlands, 'International Law in Cyberspace' 2019 (n. 15), Netherlands; see also mention in Final Report, UN OEWG, para. 18.

367 US, DHS, Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, 6 January 2017, available at: https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical; a statement by Germany in the UN OEWG suggests that it considers electoral infrastructure critical infrastructure see Germany, Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security, Comments from Germany, 6 April 2020, para. 31: 'we consider the proposals to protect the public core of the internet, not to disrupt the infrastructure essential to political processes, not to harm medical facilities and to highlight transnational infrastructure as useful additions to the already existing norms on the protection of critical infrastructure as contained in the 2015 GGE report.'

368 On electoral processes as part of the domaine réservé see above chapter 3.B.II.2.3.1.

A further contentious question is whether high governmental institutions, such as ministries or other executive bodies, should be considered critical infrastructure. The US for example designates 'government facilities' as critical infrastructure.[369] Also China designates 'e-government' and 'public services' as critical infrastructure in its Cybersecurity Act of 2017, albeit in the context of an otherwise overly broad list of critical infrastructure.[370] Designating government facilities as critical infrastructure may be prima facie plausible as e.g. the hampering of high-level ministeries or of the head of a government may affect the political stability of a state. However, the notion of governmental facilities in the cited documents cannot be sufficiently narrowed down. This eventually weighs against including governmental facilities as a distinct category of critical infrastructure under international law.

In light of the divergent definitions states and commentators have argued for a common definition of critical infrastructure. In the UN OEWG, Egypt e.g. highlighted that such a common definition could be helpful to make the prohibition to damage or otherwise impair the use and operation of critical infrastructure more effective.[371] Also Pakistan has pushed for moving forward with a definition of critical infrastructure.[372] As defining critical infrastructure is considered a confidence-building measure (CBM) in the UN OEWG Zero Report[373] it seems likely that states will continue to specify their understanding of critical infrastructure. In doing so, they

369 US, DHS, 'Statement' 2017 (n. 367).

370 Daniel Albrecht, 'Chinese Cybersecurity Law Compared to EU-NIS-Directive and German IT-Security Act', *Computer Law Review International* 19 (2018), 1–5: '[Critical information infrastructure] includes traditionally sensitive sectors such as public telecommunications and information services, energy, transportation, irrigation, finance, public services, e-government, but also includes the catch-all phrase "as well as other areas that may harm national security, the economy, and the public interest"'.

371 Egypt, Comments on the Pre-Draft report, 2020, p. 3: 'Member States should be encouraged to reach an agreed common definition of what constitutes "critical infrastructure", with a view to agreeing, as appropriate, on prohibiting any act that knowingly or intentionally utilizes offensive ICT capabilities to damage or otherwise impair the use and operation of critical infrastructure.'

372 Pakistan, Pakistan's inputs in response to the letter dated 11 March 2020 from the Chair of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (UN OEWG), p.2, para. 11.

373 UN OEWG, Zero Draft Report 2021, para. 63.

may consider a hierarchy of critical infrastructure facilities.[374] However, eventually designation of critical infrastructure is a national prerogative, as acknowledged by the UN GGE Report 2021[375] and by several states in the UN OEWG.[376] To expect a homogenous definition of critical infrastructure in the near future seems hence futile.

III. Increasing concern about harm to the public core of the internet

States have shown an increasing concern over harmful cyber operations that affect the integrity and availability of the internet.[377] In 2011 a CoE Advisory Report underlined the need to protect the internet.[378] In the Paris Call of 2018 states vowed to prevent activities that damage the general

374 Melissa Hathaway, 'Introduction: International Engagement on Cyber V: Securing Critical Infrastructure', *Georgetown Journal of International Affairs* (2015), 3–7.

375 UN GGE Report 2021, para. 44: '(…) each State determines which infrastructures or sectors it deems critical within its jurisdiction, in accordance with national priorities and methods of categorization of critical infrastructure.' para. 45: 'Highlighting these infrastructures as examples by no means precludes States from designating other infrastructures as critical, nor does it condone malicious activity against categories of infrastructures that are not specified above.'

376 Canada, Proposed norms guidance text, UN OEWG, 11 February 2021, p. 5: 'Each State determines which infrastructures or sectors it deems critical, in accordance with national priorities and methods of categorization of critical infrastructure'; Statement by South Africa at the Informal UN OEWG, 22 February 2021, p.1: '(…) the designation of national critical infrastructure and national critical information is a national competence'.

377 Dennis Broeders, *The Public Core of the Internet* (Amsterdam: Amsterdam University Press 2015), p. 11: 'The need for worldwide consensus on the importance of a properly functioning public core of the Internet seems obvious because it is these protocols that guarantee the reliability of the global Internet.'

378 The CoE Avisory Report explicitly calls for a context-specific assessment of impacts on the 'security, stability,robustness and resilience' of the internet, CoE, Steering Committee on the Media and New Communication Services (CDMC), Explanatory Memorandum to the draft Recommendation CM/Rec(2011) of the Committee of Ministers to member states on the protection and promotion of Internet's universality, integrity and openness, CM(2011)115-add1 24 August 2011, para. 51. Global Commission on the Stability of Cyberspace (GCSC), Call to Protect the Public Core of the Internet (New Delhi, November 2017), https://cyberstability.org/wp-content/uploads/2018/07/ call-to-protect-the-public-core-of-the-internet.pdf. An early proponent of identifying the public core of the Internet for special protection was Dennis Broeders, a Dutch researcher.

availability and integrity of the public core of the internet.[379] In 2019, the GCSC proposed a norm against the intentional and substantial damaging of the general availability and integrity of the public core[380], endorsed by the Organization for Security and Co-operation in Europe (OSCE) in 2019.[381] Also the UN OEWG Report and several states in the UN OEWG underlined the need to protect the integrity of cyberspace.[382] The increasing concern about harm to the public core of the internet is further evidenced by its repeated assertion as critical infrastructure.[383] The UN GGE Report 2021 for example asserted the technical infrastructure essential to the general availability and integrity of the internet as critical infrastructure.[384] This seems to suggest that harm to the public core of the internet may be conceived as a sub-category of harm to critical infrastructure. However, as harm to the public core of the internet may affect the international community as a whole – in contrast to harm to critical infrastructure

379 Paris Call (n. 11) 2018, p.3: 'To that end, we affirm our willingness to work together, in the existing fora and through the relevant organizations, institutions, mechanisms and processes to assist one another and implement cooperative measures, notably in order to: (…) Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet'.

380 GCSC, Final Report 2019, Proposed Norms, p. 21, Norm 3: 'State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace.'

381 Reiterated in OSCE, Bratislaca, Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 2019, p.20.

382 UN OEWG, Final report, para. 26: 'While agreeing on the need to protect all critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public, along with endeavouring to ensure the general availability and integrity of the Internet, States further concluded that the COVID19 pandemic has accentuated the importance of protecting healthcare infrastructure including medical services and facilities through the implementation of norms addressing critical infrastructure. such as those affirmed by consensus through UN General Assembly resolution 70/237.'

383 Germany, 'Comments' 2020 (n. 367), para. 31.

384 UN GGE Report 2021, para. 45: '(…) Critical infrastructure may also refer to those infrastructures that provide services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet. Such infrastructure can be critical to international trade, financial markets, global transport, communications, health or humanitarian action.'

which primarily affects the interests of the respective territorial state – it is preferable to distinguish the former from the latter.[385]

Regardless of this categorical question, all above-mentioned positions show a growing concern over cyber harm to the public core of the internet. This suggests that it may be considered an emerging category of significant harm under the harm prevention rule. In this vein, the CoE Report of 2011 linked the protection of the global internet to due diligence and asserted that harm to the internet may be considered significant harm.[386]

Regarding the precise protective scope of such an emerging category states, experts and commentators have either referred to the need to protect the 'general availability or integrity'[387], the public core of the internet[388], or a combination of both.[389] According to the GCSC the public core includes the 'packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, transmission media, software, and data centers'.[390] In the EU Cybersecurity Act at least 'the key protocols, the domain name system and the root zone'[391] were defined as

385 On the interest of the international community in the proper functioning of the internet see Netherlands, The Kingdom of the Netherlands' response to the pre-draft report of the UN OEWG, 2020, paras. 28, 29: '(…) adequate protection of (…) critical infrastructures would benefit the international community (…) Of this development, the internet itself is the best example (…).' On the international community as a rightholder in cyberspace, as well as on the possibility to take collective countermeasures, see chapter 5.C.IV.

386 CoE, 'Advisory Report' 2011 (n. 378), para. 78: 'This principle states that, within the limits of non-involvement in the day-to-day technical and operational matters, states should, in co-operation with each other and with all relevant stakeholders, take all necessary measures to prevent, manage and respond to significant transboundary disruptions to, and interferences with, the infrastructure of the Internet, or at any event minimise the risk and consequences arising from such events.'

387 GCSC, 'Final Report' 2019 (n. 380), norm 3.

388 The EU Cybersecurity Act, Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act), Rc. 23.

389 For an equivalent understanding of the public core and the general availability and integrity of the internet see Przemysław Roguski, 'Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea?' in Taťána Jančárková/Lauri Lindström et al. (eds.), *20/20 Vision: The Next Decade* (NATO CCDCOE 2020), 25–42, at 38, 39.

390 GCSC, 'Final Report' 2019 (n. 380), p. 31.

391 Roguski, 'Collective Countermeasures' (n. 389), 37: 'There is growing consensus that the public core of the internet should at least include the key protocols, the domain name system and the root zone, as described in the EU Cybersecurity Act.'

the public core, partially concurring with a Dutch expert report from 2016 which also determined the main protocols of the internet as the public core.[392] Hence, so far, slight divergences regarding the precise definition of harm to the public core exist. In light of the growing attention to this subject it seems plausible that states may specify their understanding of the public core in the future.

IV. Cyber espionage as a category of significant cyber harm

Cyber espionage operations are pervasive in international relations and have become a cross-cutting threat dimension across various areas. The increasing concern over the harmful effects of various forms of cyber espionage can inter alia be seen in the discussion concerning a potential prohibitive sovereignty rule in cyberspace in which proponents of the pure sovereigntist approach have underlined the harmfulness of cyber espionage[393] and in which at least one country explicitly considered espionage operations a potential violation of a prohibitive sovereignty rule.[394] In the context of the harm prevention rule the increasing concern over cyber espionage raises the question if and under which circumstances cyber espionage operations may be considered significant harm, hereby entailing a negative duty on states not to conduct such operations, as well as due diligence duties to prevent such operations by non-state actors under their jurisdiction or control.

392 Mostly focussing on the 'main protocols of the internet' Broeders, 'Public Core' 2015 (n. 377), 105: 'These new coalitions should work towards the establishment of an international norm that identifies the main protocols of the Internet as a neutral zone in which governments are prohibited from interfering for their own national interests'; 47: 'They come up with ideas for protocols and standards that regulate data transfer, interoperability, interconnection and routing between networks, and the format of the data transmitted across the Internet'.

393 Heller, 'Pure Sovereignty' 2021 (n. 190), 1499.

394 Costa Rica, 'Costa Rica's Position' 2023 (n. 243), para. 22; see above chapter 3.B.III.5.1.

1. The legality of espionage in international law

Espionage in general and cyber espionage in particular has an ambivalent role in international law.[395] On the one hand, espionage is asserted as a valuable tool for collective security[396] and for a better understanding of a state's negotiating position.[397] On the other hand, states frequently protest against espionage operations which target them and prosecute spies, while not formally objecting to each and every espionage operation.[398] Tolerance of espionage operations has been likened to the acceptance of a 'necessary evil'.[399]

The legality of espionage in international law lies in a legally grey area. Some commentators argue that extensive states practice shows that states have a right to spy[400], or that it is at least not illegal under international law as no prohibitive rule exists.[401] Other commentators argue that espionage is illegal under international law, contending that espionage violates the prohibition of intervention and territorial sovereignty.[402] Again other commentators have argued that espionage is neither legal nor illegal under international law.[403] The legality of espionage is hence at best ambiguous. In cyberspace, this result is unsatisfactory: Due to the enhanced access to devices, computer systems and content thereon, espionage operations

395 Simon Chesterman, 'Secret Intelligence', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2009), para. 3.

396 Ibid., para. 29.

397 Christopher D. Baker, 'Tolerance of International Espionage: A Functional Approach', *American University International Law Review* 19 (2003), 1091–1113, at 1104.

398 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 144.

399 Chesterman, 'Secret Intelligence' (n. 395), para. 23.

400 Asaf Lubin, 'The Liberty to Spy', *Harvard International Law Journal* 61 (2020), 185–243; Gary Brown/Keira Poellet, 'The Customary International Law of Cyberspace', *Strategic Studies Quarterly* 6 (2012), 126–145, at 133–134.

401 Stefan Talmon, 'Das Abhören des Kanzlerhandys und das Völkerrecht', *Bonn Research Papers on Public International* Law 3 (2013), at 6.

402 Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs', in Roland J. Stanger (ed.), *Essays on Espionage and International Law* (Columbus: Ohio State University Press 1962), 3 at 5, 12–13; Ian H. Mack, *Towards Intelligent Self-Defence: Bringing Peacetime Espionage in From the Cold and Under the Rubric of the Right of Self-Defence* (Sydney Law School 2013), at 4, 21–22.

403 Helmut Philipp Aust, 1. Untersuchungsausschuss der 18. Wahlperiode des Deutschen Bundestages Stellungnahme zur Sachverständigenanhörung am 5. Juni 2014, p. 14, para. 37, Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 32, p. 170.

have reached unprecedented levels in scale and scope.[404] This has made the question of the legality of cyber espionage ever more pressing.

Increasingly, commentators argue that international law prohibits cyber espionage per se[405], or at least some forms of cyber espionage operations.[406] A blanket ban of cyber espionage operations seems unrealistic but there is increasing evidence that the concern about cyber espionage has attained a cross-cutting dimension. Apart from the increasing concern about economic cyber espionage[407] this is particularly obvious with regard to bulk surveillance practices, as well as with regard to espionage operations which target governmental and international institutions.

2. Increasing concern about harm caused by mass surveillance operations

In 2013, the 'Snowden leaks' revealed the mass surveillance practices of the US intelligence service NSA. Inter alia under a programme code-named PRISM the NSA conducted foreign surveillance via spyware on individuals to collect personal data. Globally, meta and content data of individuals, as well as their communications, were intercepted and collected on an indiscriminate basis[408], inter alia through secret surveillance backdoors installed by technology companies[409], as well as through the sharing of surveillance

404 Mueller, 'Against Sovereignty' 2020 (n. 251), 788.

405 Heller, 'Pure Sovereignty' 2021 (n. 190), 1499; Buchan, 'Eye on the Spy' 2021 (n. 250): 'By penetrating computer networks and systems in order to steal confidential data, cyber espionage operations can interfere with privacy-related rights, undermine trust and confidence in digital infrastructure, disrupt the delivery of essential services and, in extreme cases, threaten national security. International law must therefore prohibit cyber espionage and deter this activity.'

406 Arguing that espionage is illegal under international law if it causes harmful effects Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 32, p. 170, para. 6; arguing that espionage is illegal under international law if it amonts to the exercise of state power, with further explanations Roguski, 'Territorial Sovereignty' 2020 (n. 133), 79.

407 See above chapter 3.C.I on economic cyber harm as a distinct category of significant harm under the harm prevention rule.

408 James Risen/Eric Lichtblau, 'How the U.S. Uses Technology to Mine More Data More Quickly', *New York Times,* 8 June 2013, available at: https://www.nytimes.com/2013/06/09/us/revelations-give-look-at-spy-agencys-wider-reach.html.

409 Talita de Souza Dias/Antonio Coco, *Cyber due diligence in international law* (Print version: Oxford Institute for Ethics, Law and Armed Conflict 2021), 79.

data of intelligence services of other countries.[410] After the revelations several states protested strongly against the mass surveillance programme and denounced its harmful impact on human rights. Resolution 68/167 of the UN General Assembly for example highlighted the detrimental impact of surveillance on the exercise and enjoyment of human rights.[411] Also the then-Brazilian president Rouseff repeatedly emphasized the harmful impact of mass surveillance on human rights.[412]

In the context of the harm prevention rule the concern about mass surveillance raises the question whether mass surveillance operations which are conducted extraterritorially, e.g. through the interception of extraterritorial data flows, can be considered significant harm. As such surveillance operations affect human rights the compatibility of such operations with human rights law comes into focus.

Before turning to this analysis it is important to note that the legality (or illegality) under human rights law is in principle without prejudice to its legal assessment as significant harm under the harm prevention rule. Hence, even if extraterritorial cyber espionage violates human rights law this does not necessarily imply that this human rights violation amounts to significant harm under the harm prevention rule. Conversely, even if extraterritorial cyber espionage is compatible with human rights law this does not preclude that it may be considered significant harm under the harm prevention rule.[413] Yet, the question whether mass surveillance violates human rights law is nevertheless relevant for the question whether it constitutes significant harm under the harm prevention rule. Art. 2 lit. b of the ILC Draft Articles on Prevention shows that harm to persons and

410 Edward Snowden: Germany a 'primary example' of NSA surveillance cooperation, *DWNews* 17 September 2019, available at: https://www.dw.com/en/edward-snowden-germany-a-primary-example-of-nsa-surveillance-cooperation/a-50452863.

411 UN General Assembly Resolution A/RES/68/167, 18 December 2013: 'Deeply concerned at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights'.

412 Statement by H.E. Dilma Rousseff at the Opening of the General Debate of the 68th Session of the UN General Assembly, 24 September 2013: 'We face (…) a situation of grave violation of human rights and of civil liberties; of invasion and capture of confidential information concerning corporate activities (…)'.

413 Such a finding could for example be based on the harmful impact of bulk surveillance programmes on the broader societal level, e.g. for consumer trust in the confidentiality of ICT products.

property infuences whether harm is significant under the harm prevention rule.[414] Furthermore, already the *Arjona* case before the US Supreme Court showed the potential link between the harm prevention rule and human rights law: The Court implicitly held that a harmful impact on the rights of individuals on the territory of another state may implicate the harm prevention rule.[415] Compliance with human rights law is hence informative for the assessment of significant harm under the harm prevention rule, but does not prejudice it.

Under international human rights law, a central issue regarding the legality of bulk surveillance is the extraterritorial scope of human rights obligations. A key question in this regard is whether extraterritorial espionage[416] is within the jurisdictional scope of human rights law.[417] Commentators had supported this argument for a long time[418] but particularly the US had advocated for a restrictive interpretation.[419] In recent years several courts have acknowledged the extraterritorial application of human rights or have at least not opposed it. The German Federal Constitutional Court for example acknowledged that the guarantee of the privacy of telecommunications also applies to extraterritorial surveillance operations.[420] The decision concerned constitutional rights under the German constitution but the Court explicitly noted the human rights law dimension of the

414 Acknowledging the relevance of human rights impacts under the harm prevention, see also ILC Draft Articles on Prevention (n. 6), art. 2b: ' "Harm" means harm caused to persons, property or the environment'.

415 US Supreme Court, *United States v. Arjona*, 7 March 1887, 120 U.S. Reports 1887, 484: 'The law of nations requires every national government to use "due diligence" to prevent a wrong being done within its own dominion to another nation with which it is at peace, or *to the people* thereof' (emphasis added).

416 I.e. intelligence practices that intercept data flows on foreign territory, e.g. via satellite.

417 For an overview of problematic jurisdictional implications of mass surveillance see Milan Tahraoui, 'Surveillance des flux de données: juridiction ou compétences de l'État, des notions à refonder', in Matthias Audit/Etienne Pataut (eds.), *L'extraterritorialité* (Paris: Pedone 2020), 141–194, at 170f.

418 Beth van Schaack, 'The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change', *International Law Studies* 90 (2014), 20–65; Helmut Philipp Aust, 'Spionage im Zeitalter von Big Data – Globale Überwachung und der Schutz der Privatsphäre im Völkerrecht', *Archiv des Völkerrechts* 52 (2014), 375–406, at 394f.

419 UN Human Rights Committee, Concluding Observations on the Fourth Report of the United States of America, adopted by the Committee at its 110th session, 10–28 March 2014, advance unedited version, para. 4.

420 BVerfG, Judgment of the First Senate of 19 May 2020, 1 BvR 2835/17, paras. 97, 98.

case.[421] In a subsequent decision the European Court of Human Rights (ECtHR) Grand Chamber avoided the question in *BigBrotherWatch* and simply assumed that extraterritorial surveillance is within a country's jurisdiction as the defendant in the case, the UK, had not raised a jurisdictional objection.[422] In *Wieder and Guarnieri v. UK* the ECtHR again avoided general remarks on the extraterritorial applicability of the ECHR. Yet, it held that interference with the data of an individual implicates the right to privacy under the convention, even if the individual is not located on the territory of the interfering state, hereby giving the judgment an undeniable relevance for the question whether the ECHR applies extraterritorially.[423] Also the Tallinn Manual assumed that cyber espionage operations could violate human rights, without however specifying under which circumstances this would be the case.[424] There are hence indicators of increasing acknowledgment of the extraterritorial applicability of international human rights law regarding privacy interferences in cyberspace, parallel to the recognition of the extraterritorial applicability of human rights law in other areas of international law, based on 'effective'[425] or 'functional' authority and control.[426]

421 Ibid.

422 ECtHR, *Case of Big Brother Watch and Others v the United Kingdom*, Grand Chamber Judgment of 25 May 2021, Applications Nos. 58170/13, 62322/14 and 24960/15, para. 272; critical in this regard Marko Milanovic, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa', *EJIL:Talk!,* 26 May 2021 available at: https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/.

423 ECtHR, *Case of Wieder and Guarnieri v. the United Kingdom*, Judgment of 12 September 2023, Applications nos. 64371/16 and 64407/16), paras. 94, 95; on the extraterritorial dimension of the case see Marko Milanovic, 'Wieder and Guarnieri v UK: A Justifiably Expansive Approach to the Extraterritorial Application of the Right to Privacy in Surveillance Cases', *EJIL:Talk!,* 21 March 2024, available at: https://www.ejiltalk.org/wieder-and-guarnieri-v-uk-a-justifiably-expansive-approach-to-the-extraterritorial-application-of-the-right-to-privacy-in-surveillance-cases/.

424 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 32, p. 170, para. 6: '[I]f cyber operations that are undertaken for espionage purposes violate the international human right to privacy (…) the cyber espionage operation is unlawful.'

425 ECtHR, *Loizidou v. Turkey (preliminary objections)*, Judgment of 23 March 1995, Application No. 15318/89, para. 88; UK Court of Appeal in the R., (*Al-Skeini) v. Secretary of State for Defence*, [2005] EWCA Civ. 1609.

426 Yuval Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law', *The Law & Ethics of Human Rights* 7 (2013), 47–71; Buchan, 'Cyber Espionage' 2018 (n. 190), 105.

On the substantive level, however, courts have so far shown leniency with regard to the outer limits of cyber espionage and have been largely deferential to states' practices. In *Big Brother Watch*, the ECtHR Grand Chamber for example rejected the argument that mass surveillance measures (on content and meta data, as well as communications) are disproportionate per se.[427] It only required that states put procedural safeguards in place, such as time limits and procedures for authorizing the selection of intercepted material, and supervision by an independent authority.[428] The ECtHR notably even stated that the collection of data did not constitute 'a particularly significant interference with privacy'.[429] This leniency tentatively weighs against the argument that bulk surveillance operations constitute significant harm under the harm prevention rule.

Aside from human rights interferences, the argument for the significance of harm caused by mass surveillance operations may however also be based on their harmful impact on the mutual trust between states. The European Commissioner for Home Affairs Malmström highlighted that the revealed mass surveillance operations harmed mutual trust and confidence between states[430] and that this may potentially affect inter-state cooperation on terrorist or criminal threats.[431] Commentators have also highlighted the broader societal harmful impacts of mass surveillance, for example on the

427 Suggesting that mass surveillance is neither necessary nor proportionate UN General Assembly Resolution A/RES/68/167, 'Right to privacy in the digital age', 18 December 2013, para. 26.

428 ECtHR, 'Big Brother Watch' (n. 422), para. 350: 'In order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "end–to–end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review.'; The judgment was criticized for its insufficient proportionality assessment see Milanovic, 'The Grand Normalization' 2021 (n. 422).

429 ECtHR, 'Big Brother Watch' (n. 422), para. 330.

430 Adrian Croft, 'EU Threatens to Suspend Data-sharing with U.S. over Spying Reports', *Reuters,* 5 July 2013, available at: https://www.reuters.com/article/usa-security-eu-idINDEE96409F20130705; on damage to mutual see also Michael Knigge, 'NSA surveillance eroded transatlantic trust', *DW*, 27 December 2013, available at: https://www.dw.com/en/nsa-surveillance-eroded-transatlantic-trust/a-17311216.

431 'EU says distrust of US on spying may harm terror fight', *BBC*, 25 October 2013, available at: https://www.bbc.com/news/world-europe-24668286.

rule of law and democractic participation, or institutional trust.[432] However, as states continue to pursue extraterritorial bulk surveillance measures, more opinio iuris would be necessary to conclude that a sufficient amount of states indeed consider such harmful impacts significant harm under the harm prevention rule. As a matter of *lex lata,* hence, cyber harm caused by mass surveillance operations cannot be considered an emerging category of significant harm under the harm prevention rule.

3. Increasing concern about cyber espionage operations against governmental and international institutions

States have furthermore increasingly expressed concern about cyber espionage operations against governmental and international institutions. In July and October 2020 the EU took restrictive measures against several individuals and the Russian intelligence service GRU which was accused of having hacked the German parliament in 2015.[433] In doing so, it based its decision on the grounds that the parliament's 'ability to operate' was 'affected', thereby causing a 'significant effect' which constituted an external threat in the meaning of Art. 1 (1) of Council Decision 7299/19.[434] It also referred to amounts of data stolen' and the compromising of email addresses.[435] While the measure was a retorsive measure and therefore not based on an alleged violation of international law it indicates that the outer limits of acceptable state behaviour had been reached in this case. As a further example of concerns about cyber espionage operations against public institutions in October 2018, the Netherlands and the UK called out Russia for an attempted hack of the Organization for the Prohibition of Chemical Weapons (OPCW) in The Hague. During the operation the Wi-fi networks were targeted through the exploitation of hardware vulnerabilities

432 Neil M. Richards, 'The Dangers of Surveillance', *Harvard Law Review* 126 (2013) 1934–1965, at 1963; Andreas Lichter/Max Löffler/Sebastian Siegloch, 'The Long-Term Costs of Government Surveillance', *Journal of the European Economic Association* 19 (2021), 741–789, at 742.

433 'Data stolen during hack attack on German parliament, Berlin says', *DW,* 29 May 2015 available at: https://www.dw.com/en/data-stolen-during-hack-attack-on-german-parliament-berlin-says/a-18486900.

434 Council of the European Union, Decision 2020/1537 (n. 159), Annex, para. 3.

435 Ibid.

at the building (i.e. a so-called close access operation).[436] The operation failed but the Netherlands, the territorial state hosting the OPCW, as well as the UK, which provided intelligence for detecting the attempt, released a statement that the operation demonstrated

> 'disregard for the global values and rules that keep us safe (…) We will uphold the rules-based international system, and defend international institutions from those that seek to do them harm'.

Additionally, cyber operations against heads of states have been condemned as violations of international law. The revelation that the phones of several heads of states, including the heads of states of Brazil, Mexico and Germany, were intercepted by the NSA for example prompted an international outcry.[437] Mexico e.g. condemned the spying of its president as 'unacceptable' and 'contrary to international law'. The concern over cyber operations against public institutions was also expressed in the UN OEWG Final Report of March 2021 which noted that:

> 'Malicious ICT activities against [critical infrastructure] and [critical information infrastructure] that undermine trust and confidence in political and electoral processes, public institutions (…) are also a real and growing concern'.[438]

It is notable that states not only protested against cyber espionage operations but also that they did so in the language of international law. In the context of the harm prevention rule it is furthermore noteworthy that when Belgium accused China of cyber espionage against its Ministry of the Interior and Defense in July 2022 it linked its concern about cyber espionage to due diligence obligations under the harm prevention rule. In what can be read as an implicit reference to the harm prevention rule it

436 'How the Dutch foiled Russian "cyber-attack" on OPCW', *BBC,* 4 October 2018, available at: https://www.bbc.com/news/world-europe-45747472.

437 UN General Assembly Resolution A/RES/68/167, 'Mexico Slams US Spying on President', *Der Spiegel,* 21 October 2013, available at: https://www.spiegel.de/international/world/mexico-condemns-reported-us-spying-by-nsa-on-president-calderon-a-929086.html quoting the Mexican foreign minister: 'This practice is unacceptable, illegitimate and contrary to Mexican law and international law'.

438 UN OEWG Final Report 2021, para. 18.

urged China to 'adhere to responsible state behavior norms (…) and to take action against such malicious activity originating from its territory'.[439]

Yet, there are also exceptions to this trend. The *SolarWinds* hack which became publicly known in December 2020 caused an international uproar.[440] Although inter alia the US Ministry of Defence was compromised the US fell short of calling out the *SolarWinds* infiltration a violation of international law. While the US imposed sanctions via an executive order[441] US president Biden merely called the operation 'inappropriate' and vowed that the US would respond in kind.[442] Beyond the *SolarWinds* example, it is also notable that the statements which invoke international law, such as the Dutch statement on the OPCW hack attempt, rarely specify legal criteria. Consequently, the legal contours of a putative legal limit of cyber espionage operations against governmental and international institutions remain unclear. The examples overall hence suggest an increasing concern about cyber espionage operations against governmental and international institutions but ambiguity as to which criteria are decisive for defining the outer limits of tolerated cyber espionage. Relevant criteria may e.g. be the importance of a public actor, interference with the operation of concerned institutions[443], significant replacement costs[444], the cumulative erosion of

439 Declaration by the Minister for Foreign Affairs on behalf of the Belgian Government urging Chinese authorities to take action against malicious cyber activities undertaken by Chinese actors, 18 July 2022, available at: https://diplomatie.belgium.be/en/news/declaration-minister-foreign-affairs-malicious-cyber-activities.

440 Patrick Beuth, 'Der Spionagefall des Jahres', *Der Spiegel,* 18 December 2020, available at: https://www.spiegel.de/netzwelt/netzpolitik/solarwinds-hack-der-spionagefall-des-jahres-a-0b728cc4-d375-4cb9-9450-3635ca8172a0.

441 US White House, 'Imposing Costs for Harmful Foreign Activities by the Russian Government', Press Release on Executive Order of 15 April 2021.

442 Ibid. Commentators have noted that the US likely conducts similar espionage operations against other countries which partially explain the reluctant reaction to the *SolarWinds* hack Jack Goldsmith, 'Self-Delusion on the Russia Hack', 18 December 2020, *The Dispatch*, available at: https://thedispatch.com/p/self-delusion-on-the-russia-hack?utm_campaign=post&utm_medium=web&utm_source=twitter.

443 Council of the European Union, Decision (CFSP) 2020/1125 of 30 July 2020, implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, Annex: 'The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work'.

444 Michael N Schmitt, 'Top Expert Backgrounder: Russia's SolarWinds Operation and International Law', *JustSecurity,* 21 December 2020, available at: https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.

public trust in such institutions[445], or the undermining of public trust in the integrity of IT.[446] As a consequence, cyber espionage operations against governmental and international institutions is thus an only cautiously emerging category of significant cyber harm.

Instead of grasping cyber espionage operations under the harm prevention rule – as e.g. Belgium has done – states may also move towards illegalizing certain forms of cyber espionage against governmental and international in the future via specific prohibitions.[447] In what could arguably be interpreted as a list of specific prohibitions of state-sponsored cyber espionage operations US President Biden sent the Russian president Putin a list of critical infrastructure targets that were 'off-limits' for attacks.[448]

V. Emerging legal yardsticks for risks of significant cyber harm

The preceding analysis has shown that several legal yardsticks for assessing whether a cyber operation amounts to a risk of significant harm can be discerned. It is clear that risks of cyber harm which – if they materialize – reach the threshold of a prohibitive rule, such as the prohibition on the use of force, the prohibition of intervention or a potential sovereignty rule, amount to risks of significant harm. Yet, it is regularly challenging to determine when the threshold of such prohibitive rules is reached. Further emerging categories of significant harm are economic cyber harm and cyber harm to critical infrastructure, as well as harm to the public core of the internet. Cyber espionage operations, such as bulk surveillance operations, or operations against governmental and international institutions, are of increasing concern in inter-state relations but the precise contours

445 On the relevance of this criterion in the context of non-intervention Germany, 'Application of International Law' 2021 (n. 68), p. 6.

446 E.g. concern regarding supply chain attacks, such as *Solar Winds*; see e.g.Written Testimony of Brad Smith President, Microsoft Corporation Senate Select Committee on Intelligence Open Hearing on the SolarWinds Hack, 'Strengthening the Nation's Cybersecurity: Lessons and Steps Forward Following the Attack on SolarWinds', 23 February 2021, p. 14: '(…) supply chain attacks that put technology users at risk and undermine trust in the very processes designed to protect them are out of bounds for state actors.'

447 Considering an illegalization of certain forms of cyber espionage in the future as a possible scenario Delerue, 'Cyber Operations' 2020 (n. 107), 200.

448 Vladimir Soldatkin/Humeyra Pamuk, 'Biden tells Putin certain cyberattacks should be 'off-limits'', *Reuters,* 17 June 2021, available at: https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16/.

of when such espionage operations amount to a risk of significant harm remain to be specified.

Chapter 4: Negative and Positive Obligations under the Harm Prevention Rule

The harm prevention rule entails two obligatory dimensions: The negative prohibitive dimension obliges states not to cause significant cyber harm.[1] The positive due diligence dimension obliges states to prevent and mitigate significant harm by non-state actors.[2]

A. The negative prohibitive dimension of the harm prevention rule

It is straightforward what states need to do to comply with the negative prohibitive dimension: They need to refrain from conducting cyber operations that cause significant harm. States for example need to refrain from cyber operations that likely cause significant economic harm or that amount to an internationally wrongful act.[3] States have highlighted the negative prohibitive dimension with regard to some categories of significant cyber harm.

I. Restrictive formulation regarding attacks on critical infrastructure in the UN GGE Reports

Regarding cyber operations against critical infrastructure the negative prohibitive dimension has received some nuance. States have underlined that critical infrastructure requires special protection under international law and should not be attacked. The UN GGE Reports stipulate a negative obligation[4] not to harm critical infrastructure

1 See chapter 2.A.VI.
2 See chapter 2.A.V.
3 On these categories of significant cyber harm see chapter 3.B and chapter 3.C.
4 The UN GGE Report introduces this obligation as a 'norm of responsible state behaviour'. On the regrettable ambiguity of this terminology in the UN GGE Reports and the preferable acknowledgment of such 'norms' as binding obligations see chapter 2.F.II.1.

> 'A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public'.[5]

The Final Report of the UN OEWG[6], the UN GGE Report 2021[7], as well as e.g. China[8] and the NAM have furthermore reiterated this negative obligation.[9] Egypt has called for a binding acknowledgement of the illegality of attacks against critical infrastructure in the UN OEWG[10] and also the African Group in the UN OEWG called for an explicit acknowledgement that cyber operations against critical infrastructure violate international law.[11] Albania and the US highlighted the norm to '[refrain] from damaging

5 United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), A/70/174, 22 July 2015 (UN GGE Report 2015), para. 13 lit.f.

6 UN OEWG Final Report 2021, para. 31.

7 United Nations, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UN GGE), A/76/135, 14 July 2021 (UN GGE Report 2021), paras. 42–46; See also UN General Assembly Resolution A/RES/73/27, 11 December 2018, para. 1.6.: 'A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.'

8 Statement by Minister-Counsellor Mr. Yao Shaojun at Arria Formula Meeting on Cyber Attacks Against Critical Infrastructure, 26 August 2020: 'The report of 2015 United Nations Group of Governmental Experts says clearly that a state should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure. However, some states still give authorization to conduct cyber attacks against critical infrastructure of other states. The practice is dangerous and does not serve the interests of all parties.'

9 UN OEWG Chairs Summary, 10 March 2021, A/AC.290/2021/CRP.3, p. 19: 'NAM stresses that all States should not knowingly conduct or support ICT activity in contrary to their obligations under international law that intentionally damages or impairs the use and operation of critical infrastructures.'

10 Remarks by Egypt at the Informal Meetings on the Zero Draft of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International security, p.1, para. 6: 'We continue to believe that there is a need for legally-binding obligations that would prohibit the use of ICTs against critical infrastructure facilities providing services to the public or for any purpose that is not consistent with International Law.'

11 Statement on Behalf of the African Group by H.E. Leon Kacou Adom, February 2021, p. 3, para. 6: '[W]e suggest to add an explicit reference that the use of ICTs to disrupt, damage, or destroy Critical Infrastructure and Critical Information Infrastructure represents a violation of International Law and the Charter obligations.'

critical infrastructure that provides services to the public'.[12] The duty not to impair critical infrastructure of other states is hence widely recognized.

The formulation of the negative obligation not to harm in the UN GGE Report is however restrictive in several aspects. First, it suggests that the negative prohibition only applies to *intentional* harm to critical infrastructure and not to accidental harm. The negative prohibitive dimension of the harm prevention rule however does not require intent in order to lead to accountability.[13] Also the Tallinn Manual acknowledged implicitly that already the causation of harmful effects may lead to the international wrongfulness of a cyber operation, regardless of intent.[14]

Second, the assertion that states should not 'conduct or knowingly support activities *contrary to [international law]* [emphasis added] that intentionally damages (…)' also suggests that intentional damage to critical infrastructure or its impairment is not *per se* contrary to international law. Such an interpretation would undermine the normative force of the rule. Statements of states indicate that the normative aim of para. 13 lit.f is precisely to prohibit attacks on critical infrastructure regardless of whether such acts violate further *distinct* rules of international law. The current formulation leaves such an interpretation however at least as a possibility.

Third, the reference to 'damage (…) or otherwise impairs the use and operation' likely excludes mere access operations (i.e. espionage operations). Access operations do not alter or delete data and hence cannot be said to cause damage or 'impair the use'. Hence espionage operations against

12 The statements followed a cyber operation which inter alia disrupted services of the Albania state police. Letter dated 7 September 2022 from the Permanent Representative of Albania to the United Nations addressed to the Secretary-General and the President of the Security Council, A/76/943-S/2022/677; US White House, Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania, 7 September 2022, available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/07/statement-by-nsc-spokesperson-adrienne-watson-on-irans-cyberattack-against-albania/.

13 Jelena Bäumler, *Das Schädigungsverbot im Völkerrecht* (Berlin: Springer 2017), p. 21; Jason D. Jolley, 'Recommendation para. 13f', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 169–190, at 188, para. 52.

14 In the context of an unintentionally harmful cyber espionage operation as a violation of sovereignty see Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press 2017), commentary to rule 32, p. 170, para. 6.

governmental institutions[15], such as in the *SolarWinds* hack, would not be covered by the negative prohibition. States are however increasingly concerned about such operations. The seemingly permissive formulation in para. 13 lit. f corresponds to the ambiguity as to the outer boundaries of espionage operations against such institutions (which in many cases can be considered critical infrastructure).[16] Only via an interpretation that would also include necessary IT replacement as disruptive cyber espionage operations against critical infrastructure would be covered under the rule. However, states have so far not adopted such an interpretation.

Therefore, while the reiteration of the negative obligation in para. 13 lit. f strengthens the normative force of the negative obligation and cements the relevance of harm to critical infrastructure as significant harm, its restrictive formulation risks to water down its protective purpose.

The UN GGE Report 2021 however at least provides some hints as to how states can avoid impairing critical infrastructure of other states. It suggested that states 'put in place relevant policy and legislative measures' to ensure compliance with the norm.[17] Such measures, seemingly akin to an impact assessment standard[18], can however so far only be considered best practice.

Aside from critical infrastructure, states have highlighted the negative obligation not to conduct harmful operation with regard to several other categories of significant cyber harm, without however providing substantially more nuance as to which activities are prohibited. Resembling the restrictive formulation of the critical infrastructure duty para. 13 lit.k of the UN GGE Report 2015 requires states not to 'conduct or knowingly support activity to harm the information systems of the authorized emergency response teams'.[19] The norm may be read as restricting potential hack-back operations. States have also highlighted the negative obligation

15 On the increasing concern over harm against governmental institutions see chapter 3.C.IV.3.

16 Ibid.

17 UN GGE Report 2021, para. 46.

18 Peter Stockburger, 'From Grey Zone to Customary International Law: How Adopting the Precautionary Principle May Help Crystallize the Due Diligence Principle in Cyberspace', in Tomáš Minárik/Raik Jakschis/Lauri Lindström (eds.) *10th International Conference on Cyber Conflict CyCon X: Maximising Effects 2018* (NATO CCD COE 2018), 245–262, at 260.

19 UN GGE Report 2015, para. 13k; on the establishment of a CERT as a due diligence requirement see below chapter 4.D.IV; see also the endorsement by Canada, Canada's Proposal for the Report of the 2019–20 United Nations Open-Ended Working Group

not to impair the public core of the internet.[20] Spain and the GCSC recommendations for example asserted that states should not launch attacks on the internet itself.[21] In a similar vein, Canada asserted in the UN OEWG that states should consider the potentially harmful effects of their activities on the 'technical infrastructure essential to the general availability or integrity of the Internet'.[22] States did not specify when an impairment of the public core would occur but it can be assumed that at least the tampering with the main protocols, potentially also via attacks on the integrity of the supply chain[23], and impairing fibre-optic or copper cables[24], would violate the negative prohibitive dimension of the harm prevention rule.

II. States' negative obligations regarding all categories of significant cyber harm

For the sake of comprehensiveness, it is to be noted that beyond the above-mentioned forms of significant cyber harm the negative prohibitive dimension of the harm prevention rule also requires states to abstain from all other forms of significant cyber harm, e.g. acts amounting to internationally wrongful acts.[25] It furthermore needs to be noted that regarding the prohibitive negative dimension the attribution problem will recur.[26] The notoriety of this problem will regularly limit the efficacy of grasping malicious state-sponsored cyber operations under the negative prohibitive dimension of the harm prevention rule.

---

on "Developments in the Field of Information and Telecommunications in the Context of International Security", 2019, p. 1.

20 On harm to the public core of the internet as a distinct category of significant harm see above chapter 3.C.III.

21 Spain highlighted attack on the internet itself as one of the main threats in cyberspace, Spain, Submission to the United Nations General Assembly Resolution A/RES/64/129/Add.1, 8 July 2009, p. 10; see also GCSC, Final Report 2019, Proposed Norms, p. 21, Norm 1: 'State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace'.

22 UN OEWG Chair's Summary, A/AC.290/2021/CRP.3, 10 March 2021, p. 13.

23 See below chapter 4.C.V.5.

24 See on the meaning of the public core of the internet chapter 3.C.III.

25 See chapter 3.B.

26 On the notorious attribution problem in cyberspace see the Introduction.

B. Required standard for due diligence under the harm prevention rule in cyberspace

Regarding the positive preventive dimension of the harm prevention rule the required standard for discharging the obligation is due diligence.[27] While due diligence is defined abstractly as a 'measure of prudence, activity, or assiduity, as is properly to be expected from, and ordinarily exercised by, a reasonable and prudent [person or enterprise] under the particular circumstances'[28] it is inherently difficult to determine what due diligence requires *in concreto*.[29] States have repeatedly called for guidance in implementing the rule.[30] The most common standard for discharging due diligence is the standard of reasonableness.[31] This standard has been endorsed by states in cyberspace, e.g. by Australia, Estonia or the Netherlands.[32]

27 See chapter 2.A.V.

28 ILA Study Group on Due Diligence in International Law, First Report, 7 March 2014, p. 19; UN Human Rights Office of the High Commissioner, *The Corporate Responsibility to Respect Human Rights: An Interpretive Guide* (United Nations 2012), p. 4.

29 Highlighting the lack of clear a content of due diligence Harriet Moynihan, 'The Application of International Law to State Cyberattacks Sovereignty and Non-intervention', *Chatham House – Research Paper*, 2019, para. 75; on the need for specification Liisi Adamson, 'Recommendation 13c', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 49–75, at 75, para. 40.

30 UN OEWG, Pre-draft Report 2020, para. 37: UN OEWG, Zero Draft 2021, paras. 32, 48; Canada, Canada's Proposal for the Report of the 2019–20 United Nations Open-Ended Working Group on "Developments in the Field of Information and Telecommunications in the Context of International Security, 2020, p. 2; Netherlands, The Kingdom of the Netherlands' response to the pre-draft report of the OEWG, 2020, p. 4; Republic of Korea, Report, 14 April 2020, p. 5. Joint comments from the EU and its Member States on the initial 'pre-draft' report of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security, 2020, p. 11, para. 32.

31 ILA Study Group on Due Diligence in International Law, Second Report, July 2016, p. 8; Anne Peters/Heike Krieger/Leonhard Kreuzer, 'Dissecting the Leitmotif of Current Accountability Debates: Due Diligence in the International Legal Order', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 1–19, 5; The ILC seemingly even equates due diligence with reasonability when it refers to the necessity of a 'reasonable standard of care or due diligence', ILC, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, UN General Assembly, Supp. No. 10, UN Doc A/56/10 (2001), commentary to article 3, para. 10.

32 Australia's Cyber Engagement Strategy, Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace, 2019,

Reasonable diligence is defined as 'such diligence as can reasonably be expected if all circumstances and conditions of the case are taken into consideration'.[33] The UN GGE Reports 2021, Canada and the UK referred to taking 'appropriate and reasonably available and feasible measures'.[34]

For assessing reasonableness in a specific case countervailing legal interests need to be taken into account. As asserted by the CoE Report 2011 the 'degree of care should be proportional to the degree of risk involved and the consequences incurred'.[35] Countervailing interests of particular importance in cyberspace are human rights obligations.[36] Risks for human rights

---

p. 91; Kersti Kaljulaid, President of the Republic at the opening of CyCon 2019, 29 May 2019, available at: https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-openingof-cycon-2019/index.html; Netherlands, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, Appendix, International Law in Cyberspace, p. 4.

33 Lassa Oppenheim, *International Law. A Treatise, Vol. II, War and Neutrality* (New York/Bombay: Longmans, Green and Co. 1906), 393.; see also Robert Sprague/Sean Valentine, 'Due Diligence', *Encyclopædia Britannica*, 4 October 2018, available at: https://www.britannica.com/topic/due-diligence.: 'The effort is measured by the circumstances under which it is applied, with the expectation that it will be conducted with a level of reasonableness and prudence appropriate for the particular circumstances.'

34 UN GGE Report 2021, para. 29: similar United Kingdom, UN GGE on Advancing Responsible State Behaviour in Cyberspace, Statement, May 2021, para. 12: 'The UK recognises the importance of States taking appropriate, reasonably available, and practicable steps within their capacities to address activities that are acknowledged to be harmful in order to enhance the stability of cyberspace in the interest of all States'; Canada, Canada's implementation of the 2015 GGE norms, Proposed norm guidance, 2019, p. 2.

35 CoE, Steering Committee on the Media and New Communication Services (CDMC), Explanatory Memorandum to the draft Recommendation CM/Rec(2011) of the Committee of Ministers to member states on the protection and promotion of Internet's universality, integrity and openness, CM(2011)115-add1 24 August 2011, para. 82; see also ILC Draft Articles on Prevention 2001 (n. 31), commentaries to art. 3, p. 154, para. 11:'The standard of due diligence against which the conduct of the State of origin should be examined is that which is generally considered to be appropriate and proportional to the degree of risk of transboundary harm in the particular instance', p. 155, para. 18: 'The required degree of care is proportional to the degree of hazard involved'.

36 UN GGE Report 2015, para. 13 lit.e: 'States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.' On the relevance of individual rights with regard to diligence measures see already Pufendorf

have for example been the reason for legitimate concerns regarding an over-extensive interpretation of due diligence in cyberspace.[37] Determining the requirements of due diligence is overall a context-dependent flexible assessment. As it is persistently difficult to determine the requirements of due diligence *ex ante*[38] a close look on a case-by-case basis is necessary to fill the abstract legal criteria with cyber-specific meaning.

I. Due diligence as a capacity-dependent binding obligation of conduct

The duty to exercise due diligence to prevent harm is an obligation of conduct.[39] It is not required that states deliver the absence of harm as a particular result. As long as a state has exercised due diligence it will not be held accountable, even if harm occurs. It is nevertheless important to note that the obligation to exercise due diligence under the harm prevention rule is a binding obligation and that its violation will entail international legal responsibility.[40] Furthermore, it is an *international* legal standard – states can hence not excuse negligence by pointing towards *diligentia in quam suis*.[41] If taking certain diligence measures is beyond a state's capacity it will however generally not be held accountable.[42] Due to greatly diverging technological ICT capacities this aspect is particularly relevant in cyberspace.[43] Yet, an objective international minimum standard of due diligence is binding for all states.[44] In the interconnected cyberspace it seems particularly important to focus on avoiding standards below this minimum

---

as depicted in Maria Monnheimer, *Due Diligence Obligations in International Human Rights Law* (Cambridge: Cambridge University Press 2021), 80.

37 See chapter 2.E.II.1.

38 Peters/Krieger/Kreuzer, 'Dissecting the Leitmotif' 2020 (n. 31), 12.

39 See chapter 2.A.V.1; see also ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment of 26 February 2007, ICJ Reports 2007, p. 43, para. 430.

40 Peters/ Krieger/Kreuzer, 'Dissecting the Leitmotif' 2020 (n. 31), 6.

41 Max Huber, *British Claims in the Spanish Zone of Morocco*, Award of 13 May 1925, vol. II, UNRIAA, 615, 644.

42 ILA, Second Report (n. 31), p. 3; implicitly affirming the relevance of a state's capacity for discharging the duty to prevent ICJ, *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgment of 24 May 1980, ICJ Reports 1980, p. 3, 32, para. 63.

43 CoE, 'Explanatory Memorandum' (n. 35), para. 77; Monnheimer, 'Due Diligence ' 2021 (n. 36), 123, 124.

44 ILC Draft Articles on Prevention 2001 (n. 31), commentaries to art. 3, p. 155, para. 17.

bottom line.[45] Above the international minimum standard higher standards may be binding on states with higher capacities. While such divergences may seem prima facie inequitable it is widely accepted in international law that diverging capacities can lead to divergent standards of accountability.[46] Hence, if a state has a certain technical apparatus, for example for intercepting communications or for shutting down servers from which harmful activities emanate, due diligence requires the respective state to use it and a state will entail international legal responsibility if it (negligently) fails to do so.[47]

II. Due diligence vs. 'soft' best practice standards

In contrast to binding standards of diligence *best practice* standards are best practices in the very meaning of the word and do not constitute binding law. They are rather soft standards to aspire to. Over time, soft best practice may harden to a binding customary standard or be incorporated into treaty law.[48] They can hereby be helpful 'halfway points'[49] in the law formation process. Informal and formal can overlap and co-exist complementarily and

45 On the relevance of the bottom line of due diligence Peters/Krieger/Kreuzer, 'Dissecting the Leitmotif' 2020 (n. 31), 12: 'The requirements of due diligence are context-dependent, often highly discretionary. In practice, the 'optimal' diligence probably never plays a role. When a dispute arises, the question is rather the bottom line. Court or other monitoring bodies will have to decide when due diligence was breached, not what would have been best'. exemplarily expressing such a bottom line *Mexico-US General Claims Commission, L. F. H. Neer and Pauline Neer (USA v. United Mexican States)*, 15 October 1926, vol. IV, UNRIAA, 60, para. 4: '[the] treatment of an alien, in order to constitute an international delinquency, should amount to an outrage, to bad faith, to wilful neglect of duty, or to an insufficiency of governmental action so far short of international standards that every reasonable and impartial man would readily recognize its insufficiency.'

46 In international climate change law, the notion of common but differentiated responsibilities e.g. informs the required standard of states' due diligence, see Lavanya Rajamani, 'Due Diligence in International Change Law', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 163–180, at 174.

47 François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press 2020), 362.

48 Hollin Dickerson, 'Best Practices', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2010), para. 21.

49 Ibid., para. 22.

interact.[50] Even if soft best practice norms do not harden to binding law they may nevertheless have a significant stabilizing effect as they induce norm adherence and cooperative state action even without, or potentially facilitated, by their non-binding character.[51] There is hence an inherent merit in collecting and assessing best practice standards. Several actors have called on a global repository of best practices regarding the implementation of the norms on responsible state behavior in the UN GGE Reports. Norway and Estonia have for example supported the establishment of a global repository to avoid fragmentation of international standards[52] and also the NAM has expressed its support.[53]

Different from soft law best practices are mere CMBs. CBMs are frequently mentioned in the UN GGE and UN OEWG Reports.[54] As the term indicates such measures aim to build confidence and to incentivize a

50 Mark A. Pollack/Gregory C. Shaffer, 'The Interaction of Formal and Informal International Lawmaking, in Joost Pauwelyn/Ramses A. Wessel/Jan Wouters (eds), *Informal International Lawmaking* (Oxford: Oxford University Press 2012) 241–270, at 242: 'More specifically, we suggest that formal and informal laws and lawmaking processes are likely to interact in a complementary fashion where distributive conflict is low, while informal and formal laws and lawmaking forums are likely to interact in competitive, antagonistic ways where distributive conflict among States is high.'

51 Dinah L. Shelton, 'Law, Non-Law and the Problem of "Soft Law"', in Dina L. Shelton (ed.) *Commitment and Compliance: The Role of Non-Binding Norms in the International Legal System* (Oxford: Oxford University Press 2000), 1–20, at 2.

52 Comments by the Norwegian Delegation on the "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security, p. 2; see also Microsoft, Submission to OEWG Draft Substantive Report, p. 2; Estonia's comments to the "Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security", 16 April 2020, paras. 1, 13, 18; China voiced concerns regarding a repository as expanding divisions and undermining trust China's Contribution to the Initial Pre-Draft of OEWG Report, p. 5.

53 Non-Aligned Movement, NAM Working Paper for the Second Substantive Session of the Open-ended Working Group on developments in the Field of Information and Telecommunications in the Context of International Security (UN OEWG), January 2021, p. 1: 'Member States should be encouraged to compile and streamline the information that they presented on their implementation of international rules and the relevant proposed repository (…)'; the establishment of a repository is mentioned as a potential CBM in the UN OEWG Chair's Summary, A/AC.290/2021/CRP.3, 10 March 2021, p. 6, para. 31.

54 UN GGE Report 2021, paras. 74–86; UN GGE Report 2015, paras. 16–18; United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013 (UN GGE Report 2013), paras. 26–29; UN OEWG Revised pre-draft, p. 8, paras. UN OEWG Final Report 2021 paras. 41–53.

cooperative dialogue.[55] Although they may partially overlap with soft law practices CBMs are preferably distinguished. Soft law still stirs normative aspirations and expectations. By contrast, the emphasis of CBMs on 'confidence' building suggests to allocate them on the level of international comity.[56]

III. Systematic interpretation of due diligence requirements in cyberspace

The international legal standard of due diligence is not to be assessed in isolation but with a view to existing standards of diligent behaviour stipulated by other primary rules of international law. The *South China Sea Arbitration* is an example of such a contextual interpretation of due diligence. In this case, the tribunal specified due diligence requirements by taking UNCLOS and international environmental law more generally into account.[57] The underlying rationale for interpreting due diligence in such a contextual manner is that standards should be interpreted systemically within the context of other rules of law.[58] The ICJ expressed this rationale well in its Advisory Opinion on the *Interpretation of Agreement* in 1980. It stated:

---

55 UN GGE Report 2021, para. 74: 'The Group notes that by fostering trust, cooperation, transparency and predictability, confidencebuilding measures (CBMs) can promote stability and help to reduce the risk of misunderstanding, escalation and conflict.'

56 Jörn Axel Kämmerer, 'Comity', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2020), para. 1.

57 Permanent Court of Arbitration, South China Sea Arbitration, Philippines v. China, Award of 12 July 2016, PCA Case No 2013–19, ICGJ p. 373–374, para. 941; on this integrative reading of due diligence Jutta Brunnée, 'Procedure and Substance in International Environmental Law', *Recueil des Cours de l'Académie de Droit International de la Haye* 405 (2020) 77–240, at 160.

58 On the desirability of coherence in the international legal order, see Anne Peters, 'The Refinement of International Law: From Fragmentation to Regime Interaction and Politicization', *International Journal of Constitutional Law* 15 (2017), 671–704; ILC, Report of the Study Group, finalized by Martti Koskenniemi, Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law, A/CN.4/L.682, 13 April 2006, p. 216, para. 430: '(…) treaties should be interpreted "in the context of the rules of international law" (…) this principle was taken for granted. Nobody challenged the idea that treaties were to be read in the context of their normative environment.' The contextual interpretation of norms in international law has also been termed as 'regime interaction', see Nele Matz-Lück, 'Norm Interpretation across International Regimes: Competences and Legitimacy', in Margaret A. Young (ed.), *Regime Interaction in International Law –*

> '[A] rule of international law, whether customary or conventional, does not operate in a vacuum; it operates in relation to facts and in the context of a wider framework of legal rules of which it forms only a part.'[59]

Similarly, the ICJ asserted in its *Namibia* Advisory Opinion:

> '[I]nterpretation and application of existing international instruments to ICTs "within the framework of the entire legal system prevailing at the time of such interpretation"'.[60]

Interpreting due diligence requirements in cyberspace hence needs to take other rules and standards of international law into account. The Czech Republic has explicitly recognized this principle for the interpretation of international law in cyberspace.[61] Also commentators have highlighted the need to interpret due diligence in light of other international legal rules and standards. The Tallinn Manual has for example been criticized for failing to take other legal regimes sufficiently into account, in particular human rights law.[62]

IV. The relevance of the duty to protect under international human rights law

Especially the duty to protect human rights may influence the required standard under the harm prevention rule. Commentators have highlighted

---

Facing Fragmentation (Cambridge: Cambridge University Press 2012), 201–234, at 209f.

59 ICJ, *Interpretation of the Agreement of 25 March 1951 Between the WHO and Egypt*, Advisory Opinion of 20 December 1980, ICJ Reports 1980, p. 73, 76, para. 10.

60 ICJ, *Legal Consequences for States of the Continued Presence of South Africa in Namibia notwithstanding Security Council Resolution 276 (1970)*, Advisory Opinion of 21 June 1971, ICJ Reports 1971, p. 16, 54, para. 118.

61 Czech Republic, Comments submitted by the Czech Republic in reaction to the initial "pre-draft" report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security, March/April 2020, para. II.iii): 'In particular, the UN OEWG could highlight the following principles, which should guide the applicability of international law in the context of ICTs: (…) interpretation and application of existing international instruments to ICTs "within the framework of the entire legal system prevailing at the time of such interpretation".

62 Antal Berkes, 'Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control', *Israel Law Review* 52 (2019) 197–231, at 219.

that the 'patchwork' of human rights obligations plays an important role for stabilizing cyberspace.[63] The particular importance of due diligence requirements under the duty to protect in international human rights law warrants a substantive depiction of international human rights law and its relation to due diligence under the harm prevention rule in cyberspace.

Unter international human rights law states have a due diligence duty to protect individuals from risks of cyber harm if the risk of harm reaches a certain significance threshold.[64] While a report of the International Law Association in 2016 had still asserted that states do not yet assume a duty to protect in cyberspace[65] states have increasingly recognized this duty in recent years[66], in particular in light of cyber incidents during the COVID-pandemic.[67] The relevance of human rights law for the harm prevention rule can already be seen in the relevance of harm to human rights for assessing the significance threshold – which inter alia takes into account

63 Antonio Coco/Talita de Souza Dias, '"Cyber Due Diligence"': A Patchwork of Protective Obligations in International Law', *European Journal of International Law* 32 (2021), 771–805, at 804: 'Thus, in a way, there is a patchwork of different but overlapping protective obligations requiring diligent behaviour in cyberspace'; affirming the applicability of international human rights law in cyberspace e.g. UN Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet, A/HRC/RES/26/13, 14 July 2014.

64 IACtHR, Case of Velásquez-Rodríguez v. Honduras, Judgment of 29 July 1988, Series C No. 4, para. 172;, ECtHR, *Case of Osman v. the United Kingdom*, Grand Chamber Judgment of 28 October 1998, Application No. 23452/94, para. 116; Björnstjern Baade, 'Due Diligence and the Duty to Protect Human Rights', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 92–108.

65 International Law Association, *Study Group on Cybersecurity, Terrorism, and International Law,* 31 July 2016, para. 71.

66 Australia, 'Cyber Engagement Strategy' 2019 (n. 32), p. 3: 'States have obligations to protect relevant human rights of individuals under their jurisdiction, including the right to privacy, where those rights are exercised or realised through or in cyberspace'; seemingly hinting also at the protective dimension under human rights law Pre-Draft Report of the UN OEWG – ICT Comments by Austria, 31 March 2020,p. 3: 'sovereignty entails rights and obligations for States, in particular with regard to the observance of human rights and fundamental freedoms, including on data protection and privacy, freedom of expression, and freedom of information.'

67 See e.g. UN GGE Report 2021, para. 71b: 'States exercise jurisdiction over the ICT infrastructure within their territory by, inter alia, setting policy and law and establishing the necessary mechanisms to protect ICT infrastructure on their territory from ICT-related threats'.

whether persons have been injured.[68] Furthermore, the due diligence duty to protect under human rights law carries several structural and doctrinal similarities with due diligence under the harm prevention rule, making its requirements particularly informative for the required standard of due diligence under the harm prevention rule. First, due diligence is also triggered by the risk of harm of a certain severity.[69] Second, once a risk of harm is objectively foreseeable[70] due diligence is triggered by the existence of a general risk to an unidentified number of individuals.[71] Third, the requirements of due diligence under the duty to protect are also assessed via a context-dependent reasonability standard.[72] States enjoy a wide margin of appreciation in fulfilling their positive obligations[73] and are only required to exercise best efforts.[74] The determination of the required due diligence furthermore takes a state's capacity and budgetary constraints into account to avoid intrusive 'micromanaging' of national institutions[75]

68 ILC Draft Articles on Prevention 2001 (n. 31), art. 2b: 'Harm" means harm caused to persons, property or the environment'.

69 ECtHR, *Case of Denisov v. Ukraine,* Grand Chamber Judgment of 25 September 2018, Application no.76639/11, para. 110.

70 Speculative risks do not suffice Baade, 'The Duty to Protect' 2020 (n. 64), Laurens Lavrysen, *Human Rights in a Positive State* (Intersentia 2017), at 131–137.

71 The IACtHR has e.g. in this regard distinguished between general and 'strict' due diligence. IACtHR, *Case of González et al. (Cotton Field) v. Mexico,* Judgment of 16 November 2009, Series C No. 205, paras 281–283; see Baade, 'The Duty to Protect' 2020 (n. 64), 98; also pointing out that the character or remoteness of the risk influences which measures need to be taken, e.g protective operational measures and providing general protection Vladislava Stoyanova, 'Fault, Knowledge and Risk Within the Framework of Positive Obligations under the European Convention on Human Rights', *Leiden Journal of International Law* 33 (2020), 601–620, 606; affirming this for the cyber context see Monnheimer, 'Due Diligence ' 2021 (n. 36), 200: 'Knowledge of [a] broad and general risk should trigger preventive obligations.'

72 ECtHR, 'Osman' (n. 64), para. 151; IACtHR, 'Velasquez Rodriguez v. Honduras' (n. 64), para 167; Baade, 'The Duty to Protect' 2020 (n. 64), 97.

73 Heike Krieger, 'Positive Verpflichtungen unter der EMRK: Unentbehrliches Element einer gemeineuropäischen Grundrechtsdogmatik, leeres Versprechen oder Grenze der Justiziabilität?', *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* 74 (2014), 187–213.

74 Helmut Philipp Aust, 'Spionage im Zeitalter von Big Data – Globale Überwachung und der Schutz der Privatsphäre im Völkerrecht', *Archiv des Völkerrechts* 52 (2014), 375–406, at 402.

75 Baade, 'The Duty to Protect' 2020 (n. 64), 101.

or a disproportionate burden.[76] Hence, several structural similarities to due diligence requirements under the harm prevention rule exist.[77]

It is however important to note that the overlap of due diligence under the harm prevention rule and due diligence for human rights protection is only partial. The main difference between both regimes lies in its protective scope. While the harm prevention rule is predominantly protecting against cyber harm manifesting extraterritorially the duty to protect under human rights law primarily aims to prevent risks of harm manifesting on a state's own territory. It only exceptionally requires to prevent risks of harm manifesting on the territory of another state.[78] Furthermore, the balancing process deviates structurally. In international human rights law proportionality balances the interests of protected individuals versus the interests of individuals affected by protective measures.[79] This is 'value-laden'[80] and structurally different from the harm prevention rule which balances the competing interests of sovereign states.

Regarding the stringency of due diligence requirements this leads to ambiguous results. On the one hand, due diligence requirements under human

76 ECtHR, *Case of Nicolae Virgiliu Tănase v. Romania*, Judgment of 25 June 2019, Application No. 41720/13, para. 136; see also Coco/Dias, 'Cyber Due Diligence' 2021 (n.63), 799; UN Human Rights Committee, General Comment No. 36 on article 6 of the International Covenant on Civil and Political Rights, on the right to life, 30 October 2018, CCPR/C/GC/36, para. 21.

77 On due diligence requirements under the harm prevention rule see above chapter 4.B.I, II.

78 Arguing for a functional approach Yuval Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law', *Law & Ethics of Human Rights* 7 (2013) 47; UN Human Rights Committee, 'General Comment 36' (n. 76), para. 63; see also Coco/Dias, 'Cyber Due Diligence' 2021 (n.63), 798; on a duty to regulate corporations with extraterritorial activities Elif Askin, 'Economic and Social Rights, Extraterritorial Application', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2019), paras. 33f.

79 Heike Krieger/Anne Peters, 'Due Diligence and Structural Change in the International Legal Order', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 351–390, at 370: '[T]he elements of the balancing process differ from those under due diligence in general international law. In human rights law, balancing may involve conflicting public interests and the human rights of other individuals. Protection against harmful activities of non-state actors in itself impacts on human rights of those others.'

80 Ibid.

rights law are arguably more demanding[81] than due diligence requirements under the harm prevention rule and may require a specific result in specific cases and hereby go beyond mere best efforts requirements.[82] On the other hand, due to the more complex balancing process, the margin of appreciation in international human rights law is an important tool for respecting democratic self-government and hence not to be interpreted restrictively.[83]

The 'family resemblance'[84] of due diligence under both regimes nevertheless requires to take human rights due diligence obligations into account when assessing due diligence requirements under the harm prevention rule, mainly for two reasons. First, taking the due diligence duty to protect into account is important to avoid fragmentation of international standards of diligence.[85] Second, taking protective duties under human rights law into account complementarily allocates risk accountability in the case of harm. If a victim state fails to diligently protect individuals under its jurisdiction against cyber harm which emanates from the territory of another state this negligence may be considered complementary contribution to the occurrence of cyber harm. As a consequence, restitution and compensation claims under the harm prevention rule may be reduced.[86]

Beyond human rights law other legal regimes, such as anti-terrorism law, telecommunications law, technical standards[87], as well as subsequent state practice regarding cybercrime treaties, may inform the required standard of 'reasonability' regarding cyber due diligence. The study will take such standards into account where appropriate.

81 Marko Milanovic/Michael Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations during a Pandemic', *Journal of National Security Law & Policy* 11 (2020), 247–284, at 281–282.

82 Krieger/Peters, 'Structural Change' 2020 (n. 79), 370.

83 Ibid.; Björnstjern Baade, *Der Europäische Gerichtshof für Menschenrechte als Diskurswächter* (Springer 2017).

84 Krieger/Peters, 'Structural Change' 2020 (n. 79), 370.

85 On the need for a systematic interpretation of due diligence which takes other rules of international law into account see above chapter 4.B.III.

86 See chapter 5.B.I.

87 UK Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015.UK, September 2019, p. 4: 'We also look to develop industry standards on security of technology, which help build cyber resilience globally. We continue to be active in the international standards space.'

V. Categories of due diligence measures

As pointed out elsewhere[88] two broad categories of diligence requirements can be discerned: Procedural due diligence obligations, and measures of institutional capacity-building. Procedural obligations are for example duties to report[89], to warn, to cooperate[90], or to assist.[91] Procedural obligations are a core part of risk management in the international legal order[92] and may be particularly important with regard to imminent and ongoing cyber incidents.

By contrast, measures of institutional capacity-building strengthen emergency preparedness[93] and resilience by providing organizational structures for risk prevention and mitigation[94], e.g. through legislative and administrative safeguard measures. Such measures are frequently instrumental for discharging procedural due diligence obligations.[95] Having for example a national computer emergency response team (CERT) can be a pre-requirement to discharge procedural due diligence obligations to assist or warn in cases of ongoing cyber operations. Similarly, it is also necessary to enact cybercrime legislation in order to diligently prosecute cyber criminals.

88 Anne Peters/Heike Krieger/Leonhard Kreuzer, 'Due diligence: the risky risk management tool in international law', Cambridge Journal of International Law 9 (2020), 121–136, 121; for an alternative framing as obligation of result (to have sufficient legislation and administrative apparatus) and an obligation of conduct (to use that capacity diligently) see Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', *Journal of Conflict & Security Law* 21 (2016), 429–453.

89 For example to report tax under the Organisation for Economic Co-operation and Development (OECD) framework; or the duty to 'prepare, communicate and maintain' successive nationally determined contributions' on greenhouse gas mitigation under art. 4.2 of the Paris Agreement in international climate change law, Rajamani, 'Climate Change Law' 2020 (n. 46), 168.

90 ILC Draft Articles on Prevention 2001 (n. 31), art. 4.

91 Highlighting the importance of procedural obligations for discharging due diligence duties of diligent harm prevention Phoebe Okowa, 'Procedural Obligations in International Environmental Agreements', *British Yearbook of International Law* 67 (1997), 275–336, at 332.

92 On the trend towards proceduralisation Peters/Krieger/Kreuzer, 'Risky risk management' 2020 (n. 88), 135.

93 ILA, 'Cybersecurity and Terrorism' 2016 (n. 65), para. 247.

94 ILC Draft Articles on Prevention 2001 (n. 31), art. 5 refers to 'necessary legislative, administrative or other action including the establishment of suitable monitoring mechanisms to implement the provisions of the present articles'.

95 On the interrelation of procedural due diligence obligations and such safeguard measures Coco/Dias, 'Cyber Due Diligence' 2021 (n.63), 804.

In the cyber context, the ITU has suggested an alternative categorisation of diligence measures and has distinguished between legal measures; technical and procedural measures; organizational structures; capacity building; international cooperation.[96] While this categorization provides an illustrative overview it mixes clearly non-binding measures, such as capacity building, with potentially legally binding diligence measures (e.g. legal measures). For the sake of greater legal clarity as to the bindingness of due diligence obligations this study will follow the distinction between procedural due diligence measures and measures of institutional capacity-building.

C. Procedural due diligence measures

I. Duty to cooperate

The necessity of international cooperation is repeatedly stressed throughout discussions in the UN GGE and UN OEWG. In the context of the harm prevention rule, this raises the question whether cooperation is a procedural due diligence requirement.

96 TU Global Cybersecurity Agenda (GCA), High-Level Experts Group (HLEG), Report of the Chairman of the HLEG (2008), available at: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx, p. 4.

1. Cooperation in international law

Inter-state cooperation is one of the purposes of the UN[97] and is essential for the maintenance of international peace and security.[98] The *Declaration on Friendly Relations and Co-Operation*[99] asserts that

> '[s]tates have the duty to co-operate with one another, irrespective of the differences in their political, economic and social systems, in the various spheres of international relations, in order to maintain international peace and security and to promote international economic stability and progress (…)'[100]

The term 'law of cooperation' (as opposed to the 'law of coordination')[101] hence expresses the necessity of coordinated state action to achieve various shared goals in modern international law. Cooperation is linked to the bona

97 Charter of the United Nations, 24 October 1945, 1 UNTS XVI, art. 1 (3): 'To achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion (…)'.

98 Ibid., art. 11 (1):' The General Assembly may consider the general principles of cooperation in the maintenance of international peace and security (…)'; art. 55, 56: '(…) United Nations shall promote: a. higher standards of living, full employment, and conditions of economic and social progress and development; b. solutions of international economic, social, health, and related problems; and international cultural and educational cooperation; and c. universal respect for, and observance of, human rights and fundamental freedoms for all without distinction as to race, sex, language, or religion' art. 56: 'All Members pledge themselves to take joint and separate action in co-operation with the Organization for the achievement of the purposes set forth in Article 55.'

99 The Declaration reflects customary international law see ICJ, *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion of 22 July 2010*, ICJ Reports 2010, p. 403, para. 80; Helen Keller, 'Friendly Relations Declaration (1970)', in Anne Peters (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2021), paras. 39, 40; Zine Homburger, 'Recommendation 13a', in Eneken Tikk (ed.) *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary,* (United Nations Office for Disarmament Affairs 2017), 9–25, at 12, para. 8.

100 UN, General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, A/RES/25/2625, 24 October 1970.

101 On the term see the seminal work of Wolfgang Friedman*, The Changing Structure of International Law* (London: Stevens 1964); on both terms as 'different techniques of legal regulation' Rüdiger Wolfrum, 'International Law of Cooperation', in Rüdiger

fide principle in Art. 2 (2) UN Charter and hence a core normative expectation inherent in international relations.[102] In various areas of international law binding duties to cooperate can be found, for example in international human rights law[103], in anti-terrorism law[104] or with regard sustainable development.[105]

2. Cooperation and due diligence

In the context of the harm prevention rule, cooperation is an essential element for discharging due diligence. Art. 4 of the ILC Draft Prevention Articles asserts a duty of cooperation with regard to the prevention of transboundary harm:

> 'States concerned shall cooperate in good faith (…) in preventing significant transboundary harm or at any event in minimizing the risk thereof'.[106]

Also the preamble, as well as ILC Draft Principles on the Allocation of Loss, reiterate a 'duty of cooperation' with regard to the prevention of transboundary harm.[107] The ILC Draft Articles on Prevention further out-

---

Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2010), paras 39–65.

102 On the link between cooperation and good faith ICJ, *Nuclear Tests (Australia v. France)*, Judgment of 20 December 1974, ICJ Reports 1974, p. 268, para. 46: 'One of the basic principles governing the creation and performance of legal obligations, whatever their source, is the principle of good faith. Trust and confidence are inherent in international co-operation, in particular in an age when this co-operation in many fields is becoming increasingly essential.'

103 International Covenant on Economic, Social and Cultural Rights in the context of business activities, E/C.12/GC/24, 10 August 2017, art. 2 (1): 'Each State Party to the present Covenant undertakes to take steps, individually and through international assistance and co-operation (…) with a view to achieving progressively the full realization of the rights recognized in the present Covenant (…)'.

104 UN, Security Council, Resolution 1373, S/RES/1373, 28 September 2001.

105 United Nations, General Assembly, Rio Declaration on Environment and Development, A/CONF.151/26, 13 June 1992, Rev.1; Principle 5: 'States and people shall cooperate in good faith and in a spirit of partnership in the fulfilment of the principles embodied in this Declaration (…).

106 ILC Draft Articles on Prevention 2001 (n. 31), art. 4.

107 ILC Draft Articles on Prevention 2001 (n. 31), preamble: 'Recognizing the importance of promoting international cooperation'; ILC, Draft Principles on the Allocation of Loss in the case of Transboundary Harm arising out of Hazardous activities,

line that a general due diligence duty to cooperate for harm prevention may entail further specific cooperative obligations[108], for example a duty to notify[109] or to conduct a risk assessment.[110] This suggests that often specific 'sub'-duties that derive from a general duty of cooperation are relevant for complying with due diligence in practice. The ICJ *Pulp Mills* case is an example of the relevance of such procedural sub-duties. In this case the ICJ analysed the interrelation between procedural obligations to inform and notify and a general obligation to cooperate with regard to shared resources. It found that cooperation is a necessary element of diligent harm prevention and highlighted that procedural sub-duties to inform and notify are necessary to discharge the broader cooperation requirement.[111] Although the Court analysed a bilateral treaty it linked its analysis to customary international law, hence indicating the relevance of its findings also beyond the analysed treaty.[112] A general-specific relationship between specific 'sub'-duties to cooperate and a general duty to cooperate can also be found in other areas of international law in which a duty to cooperate exists. In international economic law, for example, a specific duty to notify about proposed regulatory measures with significant trade effects contributes to the broader aim of 'facilitating trade through regulatory cooperation' in this area.[113]

Report of the ILC on the Work of its Fifty-Eighth Session, A/61/10, 1 May-9 June and 3 July-11 August 2006, principle 8 (3): 'States should cooperate with each other to implement the present draft principles.'

108 ILC Draft Articles on Prevention 2001 (n. 31), commentaries to art. 4, p. 155, para. 1: 'The principle of cooperation between States is essential (…) to prevent significant transboundary harm (…) More specific forms of cooperation are stipulated in subsequent articles.'

109 ILC Draft Articles on Prevention 2001 (n. 31), art. 8: If the assessment (…) indicates a risk of causing significant transboundary harm, the State of origin shall provide the State likely to be affected with timely notification of the risk and the assessment and shall transmit to it the available technical and all other relevant information on which the assessment is based.'

110 ILC Draft Articles on Prevention 2001 (n. 31), art. 7: 'Any decision in respect of the authorization of an activity within the scope of the present articles shall, in particular, be based on an assessment of the possible transboundary harm caused by that activity, including any environmental impact assessment.'

111 ICJ, *Pulp Mills on the River Uruguay Case (Argentina v. Uruguay)*, Judgment of 20 April 2010, ICJ Reports 2010, p. 14, 45, para. 101, 102.

112 Ibid.

113 See WTO/OECD, Facilitating trade through regulatory cooperation – The case of the WTO's TBT/SPS Agreements and Committees (WTO/OECD 2019), p.22.

3. Cooperation in cyberspace

In cyberspace, cooperation is frequently mentioned in the UN GGE Reports and the reports of the UN OEWG. The Guidance to the UN GGE Report 2021 stated:

> '[I]t is the common aspiration and in the interest of all States to cooperate and work together to promote the use of ICTs for peaceful purposes and prevent conflict arising from their misuse.'[114]

In his foreword to the UN GGE Report 2015 the UN Secretary-General emphasized the necessity of international cooperation to increase cyber security, hereby highlighting the vital importance of cooperation in cyberspace:

> 'Making cyberspace stable and secure can be achieved only through international cooperation, and the foundation of this cooperation must be international law and the principles of the Charter of the United Nations.'[115]

The norms of responsible state behaviour begin with a norm on cooperation which further underlines the centrality of cooperation for diligent harm prevention in cyberspace:

> 'Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.'[116]

Also France has linked cooperation to discharging due diligence in cyberspace.[117] In a reading that concurs with the above-mentioned general-specific relationship between a general normative expectation of cooperation and specific cooperative sub-duties commentators have argued that cooperation, as asserted in para. 13 lit. a, underlies also all following norms of responsible state behaviour in para. 13 lit. b–k. The underlying reason is that all norms of responsible behaviour presuppose coordinated state ac-

114 UN GGE Report 2021, para. 19.
115 UN GGE Report 2015, Foreword.
116 UN GGE Report 2015, para. 13a.
117 France, Revue stratégique de cyberdéfense, 12 February 2018, p. 86.

tion.[118] In this vein, *de Busser* has distinguished *general* cooperation under para. 13 lit. a from *specific* forms of cooperation, for example cooperation against criminal and terrorist use of cyberspace which is addressed in para. 13 lit. d.[119] A further specific area of cooperation concerns the protection of critical infrastructure which is addressed in para. 13 lit. g, lit. h.[120]

That cooperation constitutes a broad normative aspiration that also reaches into the realm of non-binding normative aspirations can be seen in both the UN GGE and the UN OEWG Reports. In both, cooperation is frequently mentioned with regard to capacity-building and CBMs.[121] The UN GGE Report 2015 even entails an own section on 'international cooperation'[122] that is tellingly disjointed from the parts on international law (Part VI) and the norms of responsible state behaviour (Part III). Cooperation is hence used in cyberspace as a catch-all term for coordinated action between states, without necessarily carrying legal weight or suggesting a binding or soft law character.

This can also be seen in cooperation references in various bilateral, regional, both binding and non-binding agreements on cybersecurity. The regional cyber security agreement of the SCO refers to cooperation in its name[123] but falls short of stipulating specific cooperative obligations. Also

118 Homburger, 'Recommendation 13 a' 2017 (n. 99), p. 10, para. 2: 'It is the basic assumption that such transboundary threats cannot be prevented and mitigated by states acting individually (…)'; Adamson, 'Recommendation 13c' 2017 (n. 29), at 72, 73, para. 35.

119 Els de Busser, 'Recommendation 13d', in Enekken Tikk (ed.), Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary (United Nations Office for Disarmament Affairs 2017), 77–94, at 77, para. 2: 'Where recommendation (a) implies cooperation between states, the purpose is to maintain international peace and security. In this sense, the purpose of recommendation (a) is directly related to the United Nations Charter and the purposes of the United Nations expressed therein.1 In general, threats to international peace and security have a different scope than that of criminal offences and terrorist activities.

120 UN GGE Report, para. 13g, h; see also below chapter 4.D.III.

121 The UN OEWG Final Report refers numerously to cooperation but notably omits references in its part on international law or norms of responsible state behaviour; cooperation is frequently referred to in the context of CBMs and capacity building, see e.g paras. 54–67, paras. 41–53.

122 UN GGE Report 2015, International cooperation and assistance in ICT security and capacity-building, Part V, para. 19–23 (Part VI on international law, Part III on norms of responsible state behavior).

123 SCO, Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security, 2009.

the SCO draft code of 2015 entails only broad cooperative expectations.[124] Further non-binding MoU on cyber security often refer broadly to cooperation[125], for example to counter malicious cyber activities[126], cybercrime[127] or cyber terrorism[128], but they also similarly fall short of specificity or bindingness. Both the generality of the references to cooperation, as well as their lack of bindingness, hence currently prevents MoUs from providing sufficiently clear normative directions as to the content of a potential diligence duty to cooperate. Consequently, it is hard to deduce meaningful normative direction from these broad assertions with regard to the potential content of a general cooperation duty under the harm prevention rule.

4. Focus on specific cooperative duties preferable

Hence, it seems advisable to be cautious to refer to a self-standing duty to cooperate as a due diligence requirement in cyberspace.[129] Frequent, or even inflationary reference to cooperation as a catch-all term, as e.g. in

124 Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/69/723, para. 1: The purpose of the present code of conduct is to (…) (4) To cooperate in combating criminal and terrorist activities that use information and communications technologies (…); (12) To bolster bilateral, regional and international cooperation, (...) to enhance coordination among relevant international organizations'.

125 Japan – Israel, Memorandum of Cooperation in the Field of Cybersecurity Between the Ministry of Economy and Industry of the State of Israel: 'Recognizing the importance of cooperation in the field of cybersecurity between Entities of both countries in sharing knowledge and information, personnel exchange or cooperative research'.

126 ASEAN-EU Statement on Cybersecurity Cooperation, 1 August 2019, para. 2: 'We underscore our commitment to promote an open, secure, stable, accessible and peaceful information and communication technology (ICT) environment, consistent with applicable international and domestic laws. We intend to strengthen our cooperation on cyber issues.'

127 U.S.-China Cyber Agreement, 16 October 2015, 'both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory (…)'.

128 United Nations Office on Drugs and Crime (UN ODC), *The use of the Internet for terrorist purposes* (United Nations 2012), paras. 73–101.

129 Highlighting that states are unlikely to accept a general duty to cooperate Wolfrum, 'Cooperation' 2010 (n. 101), para. 40. Coco/Dias leave the question open whether a general duty to cooperate in cyberspace exists, see Talita de Souza Dias/Antonio

the UN GGE Reports, or the UN OEWG Reports[130], may weaken legal clarity. It also bears the risk that cooperation becomes a convenient term for states to pay lip-service to their shared responsibility for ensuring global cybersecurity, while simultaneously evading accountability.[131]

Both in customary international law, as well as in its cyber-specific recognition, cooperation is specified through more detailed obligations, such as obligations to inform, assist, or notify, or with regard to specific areas, such as with regard to cybercrime prosecution or critical infrastructure protection. With regard to the content of due diligence requirements it seems advisable to focus on such specific cooperative obligations.

II. Duty to take action against ongoing or imminent harmful operations

During the DDoS operation against Estonia in 2007 the Estonian government notified the Russian government that harmful cyber operations were emanating from Russian territory and asked the Russian government to assist in halting the operations. The Russian government however fell short of doing so. This example evokes the question whether a refusal to cooperatively stop or mitigate an imminent or ongoing malicious cyber operation emanating from a state's territory or in case of an emergency violates the obligation to exercise due diligence.

1. Duty to take action and due diligence

Due diligence to prevent significant harm may require a state to take action against ongoing or imminent harmful operations. Art. 5 of the ILC Draft Principles on the Allocation of Loss requires the state from which harm emanates to 'ensure that appropriate response measures are taken' upon

Coco, *Cyber due diligence in international law* (Print version: Oxford Institute for Ethics, Law and Armed Conflict 2021), 242.

130 UN GGE Report 2015, International cooperation and assistance in ICT security and capacity-building, Part V, paras. 19–23 (Part VI on international law, Part III on norms of responsible state behaviour); the Final report of the OEGW e.g. refers to cooperation 27 times, while largely falling short of stipulating legal rules and norms.

131 E.g. the SCO Information Cooperation h even refers to cooperation in its title but falls short of a defining any sufficiently differentiated means of cooperation, e.g. for mutual legal assistance, for securing evidence.

the occurrence of an incident.[132] The ICJ asserted due diligence duties to take action with regard to the mitigation of imminent or ongoing harm in the *Tehran Hostages*[133] case, as well as in the *Bosnia Genocide* case.[134] Furthermore, Art. 3 of the ILC Draft Prevention Articles requires states to 'prevent significant (…) harm or at any event minimize the risk thereof'.[135] The duty to take action against imminent or ongoing harmful operations can hence be considered a core requirement for discharging due diligence under the harm prevention rule.

2. Duty to take action in cyberspace

A large number of states have recognized that they may be required to take action against harmful cyber activities. Already in 2003 the UN General Assembly asserted that states should 'act in a timely and cooperative manner (…) to respond to security incidents'.[136] In a similar vein, para. 13 lit. h of the UN GGE Report 2015 asserts that

> 'States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty'.[137]

This formulation was reiterated by the UN General Assembly[138] and the UN GGE Report 2021.[139] While the first part of para. 13 lit. h seemingly asserts a general duty to respond to harmful cyber operations against the critical infrastructure of other states, regardless of whether such operations

132 Allocation of Loss, 2006 (n. 107), principle 5b.
133 ICJ, *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgment of 24 May 1980, ICJ Reports 1980, p. 3, 12, para. 18.
134 ICJ, 'Bosnia Genocide' 2007 (n. 39), para. 431.
135 ILC, Draft Articles on Prevention 2001 (n. 31), art. 3.
136 UN General Assembly Resolution A/RES/57/239, 31 January 2003, Annex, lit. c: 'Response. Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents. They should (…) implement procedures for rapid and effective cooperation to prevent, detect and respond to security incidents.'
137 UN GGE Report 2015, para. 13 lit. h.
138 UN General Assembly Res. A/C.1/73/L.27, 22 October 2018, para. 16.
139 UN GGE Report 2021, paras. 51–55.

emanate from a requested state's territory, the second part of para. 13 lit. h addresses the classical harm prevention rule constellation in which due diligence is required from a state from which harm is emanating. The assertion in para. 13 lit. h is limited to cyber operations against critical infrastructure. Yet, several assertions of states regarding a duty to take action do not mention such a limitation. South Korea for instance merely refers to a duty to respond with regard to cyber incidents.[140] Similarly, the Netherlands and Germany broadly refer to mitigation measures regarding 'cyber attack[s]'.[141] France highlighted critical infrastructure but also asserted a duty to assist beyond acts affecting critical infrastructure.[142] Also the Tallinn Manual which takes a restrictive stance on the requirements of due diligence[143] takes the view that states are required to 'stop' ongoing or imminent attacks, regardless of whether they are aimed at the critical infrastructure of other states, as long as they reach the threshold for triggering due diligence obligations.[144] Lastly, art. 10 (4) of the Additional Protocol II to the Budapest Convention on Cybercrime requires that in the case of an emergency the requested Party 'shall respond on a rapidly expedited basis.'[145]

140 Republic of Korea, 'Comments' 2020 (n. 30), p. 5: 'When an affected State notifies another State that ICT incidents has emanated from or involve the notified State's territory with qualified information, the notified State should, in accordance with international and domestic law and within their capacity, take all reasonable steps, within their territory, to cause these activities to cease, or to mitigate its consequences.'

141 Netherlands, 'International Law in Cyberspace' 2019 (n. 32), p. 4: 'If (…) a cyberattack is carried out against the Netherlands using servers in another country, the Netherlands may, on the basis of the due diligence principle, ask the other country to shut down the servers'. Germany, Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General, Submission by Germany, A/66/152, p. 10: 'State responsibility for cyberattacks launched from their territory when States do nothing to end such attacks despite being informed about them.'

142 France, Stratégie internationale de la France pour le numérique, 2017, p. 32: '(…) adopter un comportement coopératif vis-à-vis de pays victimes d'attaques émanant de son propre territoire, par application du principe de diligence requise, en particulier lorsque l'attaque vise une infrastructure critique'.

143 See chapter 2.A.V.2.

144 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 14), commentary to rule 7, p. 43, para. 2.

145 Council of Europe, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CETS No. 224, **17 November 2021,** art.10 (4): 'Once satisfied that an emergency exists and the other requirements for mutual assistance have been satisfied, the requested Party shall respond to the request on a rapidly expedited basis.' An emergency in the meaning

Overall, there is hence overwhelming evidence that states may be required to take action against imminent or ongoing cyber operations.[146] Notably, no state has rejected a duty to stop or mitigate ongoing harmful cyber operations. Furthermore, several states have directly linked a duty to take action to due diligence under the harm prevention rule, e.g. South Korea[147], France[148] and Australia.[149]

Due to the broad references to duties to take action regarding cyber incidents there is no principled objection that in principle *any* harmful cyber operation may trigger duties to stop or mitigate harmful operations. An overly broad interpretation of such a duty can be avoided by taking both the elements of knowledge and capacity into account. But more clarity regarding states' opinio iuris would be benefitial. The hint by France in the UN OEWG that a better understanding of due diligence may help '(…) putting a stop to potential major cyberattacks'[150] indicates this need for more clarity.

3. Knowledge

With regard to the knowledge criterion the regular scenario in which a state gains knowledge, also foreseen in the UN GGE Reports, is notification by another state.[151] Several states acknowledge such constellations as well.[152]

---

of Additional Protocol II exists when 'there is a significant and imminent risk to the life or safety of any natural person, art. 3 (2c).

146 Also asserting a duty to assist Henning Christian Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge: Cambridge University Press 2020), 159; GCSC, Final Report 2019, Proposed Norms, para. 8: 'Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.'

147 Republic of Korea, 'Comments' 2020 (n. 30), p. 5.

148 France, France's response to the pre-draft report from the OEWG Chair, p. 3.

149 Australia's International Cyber Engagement Strategy, October 2017, p. 91: '[I]f a state is aware of an internationally wrongful act originating from or routed through its territory, and it has the ability to put an end to the harmful activity, that state should take reasonable steps to do so consistent with international law.'

150 France, France's response to the pre-draft report from the OEWG Chair, p. 3.

151 Karine Bannelier/Theodore Christakis, *Prevention Reactions: The Role of States and Private Actors* (Les Cahiers de la Revue Défense Nationale 2017) 32.

152 Republic of Korea, 'Comments' 2020 (n. 30), p. 5; Netherlands, 'International Law in Cyberspace' 2019 (n. 32), p. 4.

The question if also a state through which a malicious cyber operation is routed – a so-called 'transit state'[153] – shoulders a due diligence obligation has been contentious.[154] A statement by South Korea in the UN OEWG refers to due diligence obligations to assist with regard to ICT activities which 'emanate *or involve*' a state's territory[155] – which suggests that also transit states may be required to take action if they are able to. The guidance to the UN GGE Report 2021 affirms this assumption and asserts that also transit states shoulder a due diligence obligation, provided that all other conditions for due diligence obligations are met.[156]

Absent a notification, it is uncertain under which circumstances constructive knowledge can be assumed. Plausibly, a significant increase in bandwidth usage during a DDoS attack or the fact that a state regularly employs certain internet traffic monitoring mechanisms may be indicators for assuming a state's constructive knowledge of an ongoing harmful cyber operation.[157]

4. Required measures

Once a state's knowledge can be assumed, there is so far no clarity on which precise steps the respective state is required to take. The 'appropriate measures' mentioned in Art. 5 lit. b of the ILC Draft Conclusions on the Allocation of Loss are also reiterated in the statement by South Korea which

153 August Reinisch/Markus Beham, 'Mitigating Risks: Inter-State Due Diligence Obligations in Case of Harmful Cyber Incidents and Malicious Cyber Activity – Obligations of the Transit State', *German Yearbook of International Law* 58 (2015) 101–112, at 103.

154 Noting that the group of experts was split Schmitt, 'Tallinn Manual 2.0' 2017 (n. 14), commentary to rule 9, p. 55, para. 3.

155 Republic of Korea, 'Comments' 2020 (n. 30), p. 5; France, Revue stratégique 2018 (n. 117), 86.

156 UN GGE Report 2021, para. 29: 'This norm [para. 13c – the harm prevention rule reference in the UN GGE Report 2015, addition by the author] reflects an expectation that if a State is aware of or is notified in good faith that an internationally wrongful act conducted using ICTs is emanating from or transiting through its territory (…)'; extending the notion of transit state to any state affected by a botnet may risk overstretching the scope of due diligence requirements and may violate rights of individuals Lahmann Unilateral Remedies' 2020 (n. 146), 160; on general conditions for triggering due diligence requirements see above chapter 2.A.I-IV.

157 In more detail on the constructive knowledge standard in cyberspace see chapter 4.D.2.

affirms that it will take 'take all reasonable steps, within [its] territory, to cause these activities to cease, or to mitigate its consequences'.[158] The Netherlands referred to 'shut[ting] down'[159] servers which conduct a cyber attack, Australia to '[reasonable measures to put an end to harmful activities]'[160] and Germany asserted that 'do[ing] nothing' leads to state responsibility.[161] To contribute to better procedures for incident response South Korea suggested to establish a 'universal template for notification and [to] establish the relevant national point of contact'.[162] Already the UN GGE Report 2015 highlighted the benefit of 'procedures for mutual assistance in responding to incidents'[163], similar to the UN GGE Report 2021 which underlined the value of 'common and transparent processes and procedures for requesting assistance'.[164] While states have discretion to discharge the obligation[165] and a duty to stop or mitigate would in any case only be a best efforts obligation[166], it is clear that a blank refusal to cooperate would fall short of the required incident response. It is also clear that the action of CERTs will regularly be crucial for assisting with regard to cyber incidents.[167]

It may be enquired whether a state which lacks the capacity to mitigate an ongoing attack may be under a duty to request assistance from public or

158 Republic of Korea, 'Comments' 2020 (n. 30), p. 5.
159 Netherlands, 'International Law in Cyberspace' 2019 (n. 32), p. 4.
160 Australia, 'Cyber Engagement Strategy' 2017 (n. 149), p. 91.
161 Germany, A/66/152 (n. 141), p. 10.
162 Republic of Korea, 'Comments' 2020 (n. 30), p. 5.
163 UN GGE Report 2015, para. 21d: 'States should consider the following voluntary measures to provide technical and other assistance to build capacity in securing ICTs in countries requiring and requesting assistance (…) (d) Create procedures for mutual assistance in responding to incidents and addressing short-term problems in securing networks, including procedures for expedited assistance.'
164 UN GGE, Report 2021, para 54: 'Common and transparent processes and procedures for requesting assistance from another State and for responding to requests for assistance can facilitate the cooperation described by this norm (…)'; highlighting the need for more opinio iuris Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views ', *The Hague Programe for Cyber Norms – A Policy Brief,* March 2020, p. 12.
165 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 14), commentary to rule 7, p. 44, para. 6.
166 Reflecting the best efforts character of the obligation Canada, Canada's implementation of the 2015 GGE norms, 2019, p. 12; 'When Canada receives a request for assistance from another State whose CI is subject to malicious ICT acts, we respond and do our best to assist that State, and to address any threat emanating from Canadian territory.'
167 On the establishment of CERTs as a due diligence requirement see chapter 4.D.IV.

private actors. International law in some instances stipulates such duties to seek assistance. Art. 11 of the ILC Draft Articles on the Protection of Persons in the Event of Disasters for example requires states to seek assistance if a disaster 'manifestly exceeds its national response capacity'.[168] Also Art. 4 of the ILC Draft Articles on Prevention asserts that seeking assistance 'as necessary' may be required.[169] In the cyber context, the UN GGE Report 2021 referred to the possibility that a state with limited capacity 'may consider seeking assistance from other states or the private sector'[170]. Notably, Canada and Ecuador highlighted this in the UN OEWG as a possibility as well, albeit in hortatory terms.[171] As a duty to require assistance from the private sector or other states would significantly curtail state sovereignty such a duty necessarily needs to be limited to exceptional circumstances. Yet, with regard to the problem of cyber safe havens for the global stability of cyberspace a duty to request assistance, for example with regard to cyber operations that pose a risk for the life and safety of individuals or that have a significant impact on key critical infrastructure of another state, should not be excluded.[172] If such a possibility was excluded from the outset, an affected state may under certain circumstances only be able to resort to measures of self-help against the incapable state, e.g. by invoking necessity under Art. 25 ARSIWA.[173] This would arguably be even more intrusive upon state sovereignty.

168 ILC, Draft articles on the protection of persons in the event of disasters, with commentaries, Yearbook of the International Law Commission, 2016, vol. II, Part Two, art. 11: 'To the extent that a disaster manifestly exceeds its national response capacity, the affected State has the duty to seek assistance from, as appropriate, other States, the United Nations, and other potential assisting actors.'

169 ILC Draft Articles on Prevention 2001 (n. 31), art. 4: 'States concerned shall cooperate in good faith and, as necessary, seek the assistance of one or more competent international organizations', commentary to art. 4, p. 156, para. 6: 'The principle of cooperation means that it is preferable that such requests be made by all States concerned. The fact, however, that all States concerned do not seek necessary assistance does not free individual States from the obligation to seek assistance (…)'.

170 UN GGE Report 2021, para. 30b.

171 UN OEWG Chair's Summary, A/AC.290/2021/CRP.3, 10 March 2021, p. 12 (Canada), p. 18 (Ecuador).

172 Monnheimer, 'Due Diligence ' 2021 (n. 36), 121.

173 Arguing that self-help measures may be justified by necessity, however in very limited circumstances Lahmann, 'Unilateral Remedies' 2020 (n. 146). 204f., 255.

5. Widespread support of a due diligence obligation to take action in cyberspace

Therefore, the duty to take action against imminent and ongoing cyber operations has found widespread support by states and commentators.[174] States are well advised to further specify the precise contours of when assistance obligations are triggered, under which conditions knowledge can be presumed, and which precise measures are to be taken.[175] Operational templates for incident response may significantly contribute to clarifying required standard. A duty to take action in cases of emanating harm can be considered a key procedural due diligence requirement. As was pointed out by *Milanovic/Schmitt:* '[W]hy would any responsible state not take feasible measures to put an end to [harmful] activity'[176]?

III. Duty to notify

A further procedural due diligence requirement may be a duty to notify other states about known risks of harm.

1. Duty to notify in international law and with regard to due diligence

In international law duties to warn in emergency situations exist in numerous treaties, such as with regard to oil pollution[177], nuclear incidents[178], in the law of international watercourses[179], or for the protection of human rights.[180] Also the ILC Draft Articles on Prevention assert a duty to warn in

174 Bannelier/Christakis, 'Prevention Reactions' 2017 (n. 151) 32.
175 Roguski, 'Comparative Analysis' 2020 (n. 164), 12.
176 Schmitt/Milanovic, 'Cyber (Mis)information' 2020 (n. 81), 281.
177 International Convention on Oil Pollution Preparedness, Response and Cooperation, 30 November 1990, 1995 UNTS 78, art. 5 lit.c.
178 Convention on Early Notification of a Nuclear Accident, 26 September 1986, 1439 UNTS 275, art. 5.
179 Convention on the Law of the Non-navigational Uses of International Watercourses of 21 May 1997, 2999 UNTS, art. 28.
180 ILC, 'Draft Articles Disasters' (n. 168), art. 3a: 'For the purposes of the present draft articles: (a) "disaster" means a calamitous event or series of events resulting in widespread loss of life, great human suffering and distress(…)'; art. 9 (2): 'Disaster risk reduction measures include the conduct of risk assessments, the collection and

the case of an emergency.[181] Beyond treaty law international tribunals have asserted a duty to warn about dangers in their territory.

First, in a passage in *Trail Smelter* case the Tribunal already asserted a duty to warn in case an emission reached a certain threshold.[182] It is not clear if the Tribunal based its finding on domestic or international law but the link between warning and harm mitigation already became evident. In the *Corfu Channel* case in which Albania failed to warn the UK of mines in its territorial sea Judge *Alvarez* poignantly asserted in his Separate Opinion:

> '[A] State is bound to give immediate information to countries that are concerned regarding the existence in its territory of dangers, resulting from the action of other States, that have been brought to its knowledge, and which might cause injury to the said countries'[183]

The court's stance in *Corfu Channel* is noteworthy as it makes clear that a duty to warn is based on 'elementary considerations of humanity', hereby indicating that the reasoning is of a general character and not restricted to a specific area of international law.[184] The judgment furthermore makes clear that warning about risks of harm may be required under due diligence for harm prevention. Although the case did not explicitly refer to due diligence this was the undercurrent of the decision.[185] Beyond the Draft Prevention Articles the ILC has also underlined the importance of warning in its Draft Principles on the Allocation of Loss[186], as has the UN Security Council

---

dissemination of risk and past loss information, and the installation and operation of early warning systems'.

181 ILC Draft Articles on Prevention 2001 (n. 31), commentary to art. 17: 'The State of origin shall, without delay and by the most expeditious means, at its disposal, notify the State likely to be affected of an emergency concerning an activity within the scope of the present articles and provide it with all relevant and available information.'

182 *Trail Smelter Case (United States v. Canada)*, Decisions of 16 April 1938 and 11 March 1941, vol. III, UNRIAA, 1905–1982, at 1970.

183 ICJ, *Corfu Channel Case (United Kingdom v. Albania)*, Judgment of 9 April 1949, Separate Opinion of Judge Alvarez, ICJ Reports 1949, p. 39, 45, para. 6; concurring with the judgment, Judgment of 9 April 1949, p. 23.

184 Okowa, 'Procedural Obligations' 1997 (n. 91), 331.

185 Krieger/Peters, 'Structural Change' 2020 (n. 79), 357. The ILC Allocation of Loss principle; makes clear that the duty to warn in itself is also a due diligence obligation, see Allocation of Loss, 2006 (n. 107), commentary to principle 5, p. 167, para. 2.

186 Allocation of Loss, 2006 (n. 107), principle 5a: 'Upon the occurrence of an incident involving a hazardous activity which results or is likely to result in transboundary

with regard to the prevention of terrorist acts.[187] A duty to warn about harmful activities was reiterated by the ICJ in Nicaragua as well.[188] A duty to warn about risks of harm emanating from a state's territory is hence firmly anchored in international law and a recognized procedural sub-duty of due diligence.

2. Duty to notify in cyberspace

In cyberspace, the existence of early warning systems for malicious cyber operations against critical infrastructure was already mentioned in UN General Assembly Res. 58/199 in 2004.[189] Also commentators have underlined its stabilizing value.[190] Yet, so far, states have acknowledged a duty to notify only lukewarmly. A CoE Report of 2010 acknowledged a duty to provide timely notification about threats to the general integrity of the internet.[191] Ecuador acknowledged that informing another state of a harmful activity may be required to discharge due diligence, but did so in notably hortatory terms.[192] Also the Joint Statement of Russia and

damage: (a) the State of origin shall promptly notify all States affected or likely to be affected of the incident and the possible effects of the transboundary damage'.

187 UN, Security Council, Resolution 1373, S/RES/1373, 28 September 2001, para. 2b: 'States shall (…) (b) Take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information.".

188 ICJ, *Military Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment of 27 June 1986, ICJ Reports 1986, p. 14, 103, para. 215.

189 UN General Assembly Resolution A/RES/58/199, 23 December 2003, Annex Elements for protecting critical information infrastructures, para. 1: 'Have emergency warning networks regarding cyber-vulnerabilities, threats and incidents.'

190 Arguing for a duty to notify with regard to cyber espionage Heike Krieger, 'Krieg gegen anonymous', *Archiv des Völkerrechts* 50 (2012), 1–20, at 8.

191 Interim report of the Ad-hoc Advisory Group on Cross-border Internet to the Steering Committee on the Media and New Communication Services incorporating analysis of proposals for international and multi-stakeholder co-operation on cross-border Internet, H/Inf (Council of Europe 2010), p. 21, para. 91f.: 'states should take all reasonable measures to provide prior and timely notification and relevant information to states that may be potentially affected [by disruption to or interferences with the stability and resilience of Internet resources, addition by the author].'

192 Ecuador preliminary comments to the Chair's "Initial pre-draft" of the Report of the United Nations Open Ended Working Group on developments in the field of information and telecommunications in the context of international security (UN

China[193] which refers to 'information-sharing' seems at this point as a mere normative aspiration. While India acknowledged the relevance of early warning for cyber threats against critical infrastructure[194] it fell short of further endorsing a duty to warn but rather allocated warning mechanism as a CBM. Early warning mechanisms were also mentioned as a CBM by China.[195] A general duty to warn about risks of cyber harm is notably absent throughout statements of states and in the work of the UN GGE and the UN OEWG. Overall, states have hence avoided to commit to an obligation or responsibility to notify. Yet, it is also noteworthy that states have not explicitly rejected a duty to notify.

3. Reluctance of states to commit to a duty to notify in cyberspace

A reason for the reluctance of states may inter alia be that the disclosure of information may reveal a state's intelligence capacities.[196] Art. 14 of the ILC Draft Prevention Articles acknowledges that national security interests may be an interest which limits a state's duty to notify.[197] The reluctance

OEWG), p. 2: 'State identifies malicious cyber activity emanating from another State's region or cyberinfrastructure, a first step could be notifying that State.'

193 The Joint Statement Between the Presidents of the People's Republic of China and the Russian Federation on Cooperation in Information Space Development, 26 June 2016, para. 7: 'Advance cooperation in information security emergency response and information sharing of information security threat, and enhance cross-border information security threat management'.

194 India, Latest Edits to Zero Draft, 2021, p. 14, para. 88: 'Information sharing and coordination at the national, regional and international levels can make capacity-building activities more effective, strategic and aligned to national priorities.

195 Statement Yao, 'Critical Infrastructure' 2020 (n. 8): 'States should (…) explore the possibilities to establish relevant risk early warning and information sharing mechanism (…)'.

196 Oren Gross, 'Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents', *Cornell International Law Journal* 48 (2015), 481–511, at 504.

197 ILC Draft Articles on Prevention 2001 (n. 31), art. 14: 'National security and industrial secrets Data and information vital to the national security of the State of origin or to the protection of industrial secrets or concerning intellectual property may be withheld, but the State of origin shall cooperate in good faith with the State likely to be affected in providing as much information as possible under the circumstances.' In the context of the ILC draft prevention articles this caveat applies to information to the public (in Art. 13) but the rationale similarly applies to notification to other states.

of states may furthermore be due to the lack of certainty under which circumstances a duty to inform may be triggered. It is not fully clear to whom a duty to warn would be owed. On the one hand, it is relatively clear that it would cover states which are affected, or potentially affected by a harmful operation.[198] On the other hand, a duty to warn may extend to a duty to warn the public about dangers. The UN OEWG notably mentions the notification of users about ICT vulnerabilities as a CBM.[199] Moreover, para. 13 lit. j of the UN GGE Report 2015 is primarily addressed at disclosure of vulnerabilities to the public.[200] Also the 2010 CoE Advisory Report highlights that information sharing on ICT vulnerabilities between private actors is an important aspect for ensuring cyber resilience of critical infrastructure.[201] Informing the public likely affected by harmful activities is foreseen in Art. 13 of the ILC Draft Prevention Articles as well.[202]

The repeated emphasis on information to the public evokes the question whether such a duty could be conceived as a requirement under the harm prevention rule or whether it should rather be conceived as a protective duty under human rights law. Statements of states so far do not clarify the legal basis for informing the public and individuals. The more plausible claim is that a duty to notify and inform the public is a due diligence requirement only under the duty to protect in international human rights law as it is acknowledged that notification with regard to grave risks can be required under international human rights law.[203] By contrast, the harm

198 Ecuador, 'Preliminary comments' 2020 (n. 192), ILC Draft Articles on Prevention 2001 (n. 31), art. 8 (1).

199 UN OEWG, zero draft, para. 50; revised draft, para. 42, initial draft para. 38.

200 UN GGE Report 2015, para. 13j: 'States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.' See in more depth on disclosure of vulnerabilities in chapter 4.C.V.3. For an alternative reading that it may be also require reporting to other states in the light of the due diligence rationale see Nicholas Tsagourias, 'Recommendation 13j', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 241–264, p. 261, para. 36.

201 Ad-hoc Advisory Group on Cross-border Internet, 'Interim Report' 2010 (n. 201), p.21, para. 91.

202 ILC Draft Articles on Prevention 2001 (n. 31), art. 14.

203 ECtHR, *Case of Budayeva and Others v. Russia*, Judgment of 20 March 2008, Application Nos 15339/02 et al., para. 162, 176; Baade, 'The Duty to Protect' 2020 (n. 64), 103.

prevention rule, as an inter-state obligation, is owed primarily to affected states, but not to individuals or the general public. Nevertheless, the mention of information to the public in the part of the UN GGE Report on norms of responsible state behaviour at least suggests that it can also be in the interests of other states that the public – which may also include other states – is informed.[204]

States have so far not specified the procedure and timing for diligence duties to warn in cyberspace. Under customary international law it is clear that the notification has to follow immediately upon acquiring knowledge[205], in the case of disasters 'without delay and by the most expeditious means'.[206] Furthermore, it should include 'all relevant and available information'.[207] With regard to contact points the now-repealed EU Directive on the security of network and information system (NIS Directive) exemplarily asserted that it should go through trusted channels.[208] It may moreover be considered good practice to include information of the scope and gravity of the risk of harm.[209]

4. Nascent emergence of a due diligence obligation to notify in cyberspace

There are strong reasons to assume a duty to notify other states about impending attacks exists.[210] While general rules on due diligence for harm prevention strongly support such a duty the reluctance of states and their tentative relegation of notification to the level of capacity building or CBMs so far weakens the normative pull of such a diligence requirement in cyber-

204 See Tsagourias, 'Recommendation 13j' 2017 (n. 200), para. 36.

205 ILC Allocation of Loss, 2006 (n. 107), commentary to principle 5, p. 167, para. 2: 'The notification obligation has to be performed as soon as it is practicable'. Okowa, 'Procedural Obligations' 1997 (n. 91), 295.

206 ILC Draft Articles on Prevention 2001 (n. 31), art. 17.

207 Ibid.

208 EU, Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS 1 directive), para. 59.

209 As e.g. foreseen in ILC Draft Articles on Prevention 2001 (n. 31) art. 13.

210 See also Gross, 'Cyber Responsibility' 2015 (n. 196), 503; Adamson, 'Recommendation 13c' 2017 (n. 29), p. 72, 73, para. 35: 'Exchange of information is an essential facilitating element of effectively exercising due diligence. It covers inter alia the exchange of information about risks of significant transboundary harm with the potentially affected parties, potential threats in general, information about vulnerabilities, as well as sharing information for the investigation and prosecution purposes.'

space. A due diligence obligation to notify about risks of cyber harm is hence only nascently emerging. Similar to other potential due diligence requirements the lack of a sufficiently precise legal content seems to inhibit states to commit to a duty to notify, potentially due to concerns to expose intelligence capabilities. States are well advised to be more forthcoming with regard to their opinio iuris. Best practice templates may provide a stabilizing next step towards the evolution of an international legal standard.

IV. Duty to cooperate on the prosecution of cybercrime

A study by the European Commission in 2018 found that more than half of cybercrime investigations involve a transnational element.[211] Accessing and securing relevant evidence stored abroad is however difficult due to enforcement jurisdiction limits. In principle, it is the exclusive right of the territorial state to access data stored on its territory for law enforcement purposes. As a consequence, international cooperation for securing evidence and for apprehending perpetrators is necessary.[212] While efficient cooperation presupposes institutional safeguards[213] the main emphasis of cooperation with regard to prosecution of cybercrime lies on procedures for coordinated action. It is hence discussed here as a potential *procedural* due diligence obligation.

211 European Commission Staff Working Document, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceeding, 17 April 2018, SWD/2018/118 final; see also Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation', *Monash University Law Review* 40 (2015), 698–736, at 700.

212 Theodore Christakis/Fabien Terpan, 'EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options', *International Data Privacy Law* 11 (2021), 81–106; Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations Under International Law* (Intersentia 2014), 30.

213 See below chapter 4.D.I.on cybercrime legislation as a due diligence requirement.

1. Prohibition of extraterritorial law enforcement as a challenge for cybercrime prosecution

The collection of evidence on servers located abroad without the consent of the territorial state regularly violates the exclusive right of territorial law enforcement of the territorial state.[214] The only mechanism by which the consent of the territorial state can be sidelined are direct access procedures which enable law enforcement agencies to directly request data from private service providers. Yet, such procedures, as e.g. foreseen in Art. 32 lit. b of the Budapest Convention on Cybercrime[215], are so far limited to like-minded countries. Due to the stance of several countries on 'sovereign control' over national cyberspace and the challenges of securing due process safeguards regarding direct access this is unlikely to change.[216] Current attempts to legalize direct access to private service providers for obtaining evidence, circumventing the mutual legal assistance process, have also been criticized as a potential 'race to the bottom' for human rights safeguards.[217]

214 UN ODC, Comprehensive Study on Cybercrime, February 2013, p. 184; Michael Schmitt/Liis Vihul, 'Respect for Sovereignty in Cyberspace', *Texas Law Review* 95 (2017), 1639–1670, at 1660; on the exclusive right to exercise state power Przemysław Roguski, 'Violations of Territorial Sovereignty in Cyberspace – an Intrusion-Based Approach', in Dennis Broeders/Bibi van den Berg (eds.), *Governing Cyberspace: Behaviour, Power and Diplomacy* (London: Rowman & Littlefield 2020), 65–84, at 74, inter alia referring to PCIJ, *The Case of the S.S. Lotus (France v. Turkey)*, Judgment of 7 September 1927, Series A, No. 10, p. 4 at 18, 19: '[F] ailing the existence of a permissive rule to the contrary [a State] may not exercise its power in any form in the territory of another State'.

215 Council of Europe Convention on Cybercrime, 23 November 2001, ETS 2001, No. 185, art. 32 lit.b: 'A Party may, without the authorisation of another Party (…) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.'

216 Russia e.g. fiercely opposes Art. 32 lit. b of the Budapest Convention as it views it as a violation of state sovereignty, see EDRI, 'Transborder data access: Strong critics on plans to extend CoE Cybercrime Treaty', 5 June 2013, available at: https://edri.org/our-work/edrigramnumber11-11transborder-data-access-cybercrime-treaty/.

217 EDRI, New Protocol on cybercrime: a recipe for human rights abuse?, 25 July 2018, available at: https://edri.org/our-work/new-protocol-on-cybercrime-a-recipe-for-human-rights-abuse/; the EU Draft Production Order hence foresees the non-execution of Production Orders if the private service provider considers that compliance with a production order would violate the law of a third state, e.g. fundamental rights stipulated in the law of the third's state, see EU, Proposal for a Regulation of the European Parliament and of the Council on European

Therefore, inter-state cooperation, in particular with regard to the securing and accessing of digital evidence, is key to efficient cybercrime prosecution.[218]

2. Cooperation in legal instruments on cybercrime: Discussions on the UN level

On the UN level, the necessity of cooperation with regard to cybercrime is repeatedly stressed in resolutions of the UN General Assembly[219] It has also featured prominently in the negotiations of an international convention on cybercrime.[220] States have not directly linked cooperation on cybercrime to due diligence but an integrative reading of the norms of responsible state behaviour[221], including the general cooperative aspiration in para. 13 lit. a[222], suggests that cooperation for cybercrime can be conceived as part of the diligence required under para. 13 lit. c of the UN GGE Report 2015. Yet, the UN GGE assertion regarding cooperation on cybercrime prosecution is poignantly hortatory. Para. 13 lit. d of the UN GGE Report of 2015 broadly stipulates that:

> 'States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may

Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final – 2018/0108 (COD), 17 April 2018, art. 15, 16.

218 See also UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 183f.

219 See already UN General Assembly Resolution A/RES/58/199, 23 December 2003, Annex, para. 10: 'Engage in international cooperation, when appropriate, to secure critical information infrastructures, including by (…) coordinating investigations of attacks on such infrastructures in accordance with domestic laws.'

220 See UN GA, Ad Hoc Committee to Elaborate a Comprehnsive International Convention on Countering the Use of Information and Communictions Technologies for Criminal Purposes, A/AC.291/22, 29 May 2023, art. 35 (1): 'States Parties shall cooperate with each other in accordance with the provisions of this Convention, as well as other applicable international instruments on international cooperation in criminal matters (...).'

221 Homburger, 'Recommendation 13 a' 2017 (n. 99), p. 10, para. 2; see also above chapter 4.B.III.

222 See above chapter 4.C.I.

> need to consider whether new measures need to be developed in this respect'.[223]

In slightly more assertive language the UN GGE 2013 notably stated that:

> 'States should intensify cooperation against criminal or terrorist use of ICTs, harmonize legal approaches as appropriate and strengthen practical collaboration between respective law enforcement and prosecutorial agencies'.[224]

The poignantly hortatory language of the UN GGE Reports hence entails little normative substance and is more akin to an optimization aspiration than to a firm legal commitment. Also the assertion that states may resort to voluntary agreements on cybercrime cooperation as a non-binding CBM underlines that the UN GGE Reports largely relegate cybercrime cooperation to the level of non-binding norms:

> 'States should consider additional confidence-building measures that would strengthen cooperation on a bilateral, subregional, regional and multilateral basis. These could include voluntary agreements by States to: (…) (e) Cooperate, in a manner consistent with national and international law, with requests from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.'[225]

3. Cooperation requirements in cybercrime treaties

A reason for the reluctance of states in the UN GGE Report inter alia may be that states want to avoid contradictions or frictions with cooperation requirements under regional cybercrime treaties. Several binding cybercrime

223 UN GGE Report 2015, para. 13 lit. d; on the implementation of para. 13 lit.d see UN GGE Report 2021, para. 32: 'Observance of this norm implies the existence of national policies, legislation, structures and mechanisms that facilitate cooperation across borders on technical, law enforcement, legal and diplomatic matters relevant to addressing criminal and terrorist use of ICTs.' Para. 33: '(…) States are also encouraged to develop appropriate protocols and procedures for collecting, handling and storing online evidence relevant to criminal and terrorist use of ICTs and provide assistance in investigations in a timely manner, ensuring that such actions are taken in accordance with a State's obligations under international law.'

224 UN GGE Report 2013, para. 22.

225 UN GGE Report 2015, para. 17 lit.d.

treaties stipulate duties to cooperate on cybercrime prosecution.[226] Art. 23 of the Budapest Conventions e.g. stipulates that states shall cooperate to the widest extent possible in criminal matters and with regard to mutual legal assistance requests.[227] Similarly, Art. 34 of the Arab League Convention stipulates cooperation requirements and procedures regarding mutual legal assistance.[228] Furthermore, several non-binding MoU entail agreements to cooperate in cybercrime prosecution. For example, the MoU between China and the US of 2015 asserts that both states '[agree to cooperate with regard to requests to investigate cybercrimes]'.[229] Further similar MoUs on cooperation exist, frequently reiterating the intent to cooperate on cybercrime without further specification.[230]

Overall, hence, a wide net of binding and non-binding cooperation norms regarding cooperation on prosecution of cybercrime exists, underlining that cooperation for cybercrime is regularly a normative expectation in international law. Regarding the complexity of the wide net of binding and non-binding cooperation norms it however remains the question

226 On cybercrime legislation as a due diligence requirement see below chapter 4.D.I.

227 Convention on Cybercrime 2001 (n. 215), art. 23: 'The Parties shall co-operate with each other (…) to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.' See also ibid., art. 25: 'The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence'.

228 Arab League, Convention on Combating Information Technology Offences, 21 December 2010, art. 34 (6): 'The State Party from which assistance is requested shall commit itself to inform the requesting State Party of the result of the implementation of the request. If the request is refused or postponed, the reasons of such refusal or postponement shall be given. The State Party from which assistance is requested shall inform the requesting State Party of the reasons that prevent the complete fulfillment of the request or the reasons for its considerable postponement.'

229 However, under the precondition that cooperation requirements comply with domestic law, see U.S.-China Cyber Agreement, 16 October 2015: 'The United States and China agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities. Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory.'

230 E.g. ASEAN-EU, 'Statement' 2019 (n. 126), para. 11; Memorandum of Understanding between the Government of the Republic of Indonesia and the Government of Australia on Cyber Cooperation, 31 August 2018, para. 2 (4).

whether an objective minimum standard as a bottom line and least common denominator can be deduced as a binding due diligence requirement.

4. Tracing international legal standards for cybercrime cooperation

There are two main tracks of cooperation on cybercrime prosecution: Formal cooperation, mainly in the form of mutual legal assistance requests, and informal cooperation, through direct law enforcement cooperation, agency-agency cooperation or cooperation between liaison officers.[231]

4.1 Formal cooperation: Mutual legal assistance

Formal cybercrime cooperation is primarily channelled via mutual legal assistance. Mutual legal assistance is no general obligation under international law but is stipulated by a variety of mutual legal assistance treaties, mostly on a bilateral and in some cases regional level. Such regional and bilateral mutual legal assistance treaties in criminal matters often exist alongside treaties on administrative mutual legal assistance, and treaties on civil and commercial legal assistance.[232] The function of mutual legal assistance is to make cooperation in criminal prosecution more timely and more reliable and to facilitate direct contact between judicial authorities.[233] The treaties for example address securing and obtaining evidence, or the apprehension and extradition of persons.[234] Due to the increasing transnational dimension of various criminal activities, for example human trafficking, the importance of mutual legal assistance in international relations has been growing.

With regard to cybercrime the Budapest Convention and the Arab League Convention stipulate specific rules for mutual legal assistance in inves-

231 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 187.

232 Dieter Martiny, 'Mutual Legal Assistance in Civil and Commercial Matters', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2009), para. 1f.

233 Time René Salomon, 'Mutual Legal Assistance in Criminal Matters', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2013), para. 11.

234 See Convention on Cybercrime 2001 (n. 215), art. 24, Arab Convention (n. 228), art. 31; UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 199.

tigations[235], but also general mutual legal assistance treaties may apply to cybercrime investigations.[236]

4.2 Principles and limits of mutual legal assistance

Important principles of mutual legal assistance are the principle of reciprocity, dual criminality and mutual recognition.[237] A state will only take law enforcement measures after a mutual legal assistance request if it considers the conduct in question criminal as well. As states homogeneously criminalize core cyber offences against the confidentiality, integrity and availability of ICT[238] the issue of dual criminality is not insurmountable regarding cyber harm.[239] Yet, mutual legal assistance agreements entail multiple reasons which allow a state to reject a request. A state may for example refuse requests due to incompatibility with domestic law, e.g. with constitutional rights. In the cyber context, a state can for instance refuse a request due to its incompatibility with privacy or data protection rules. In this regard, the problem that states' standards and safeguards for protecting individual rights diverge becomes acute.[240] Furthermore, states may refuse requests due to national security concerns or essential security interests of a state, as can for example be seen in the ICJ case in *Djbouti vs. France*.[241] Also the Budapest Convention entails a provision recognizing that 'it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests'.[242] Ultimately, mutual legal assistance depends to a significant extent on the political will

235 See Convention on Cybercrime 2001 (n. 215), art. 24, Arab Convention (n. 228), arts. 34, 39, 41, 42.

236 Clough, 'Challenges of Harmonisation' 2015 (n. 211), 731.

237 On the importance of the dual criminality rule see UN ODC, 'Comprehensive Study' 2013 (n. 214), p.60.

238 See on converging standards regarding key cybercrime offences in more detail below chapter 4.D.I.4.2. However, with regard to content crimes, this is likely to be different.

239 Under the Budapest Convention states are encouraged to apply a flexible approach when applying dual criminality, see Explanatory Report to the Convention on Cybercrime, 23 November 2001, para. 259.

240 See on diverging safeguards and standards of in criminal procedural law, e.g. regarding time limits, judicial review, or limited list of offences chapter 4.D.I.5.2.

241 ICJ, *Case Concerning Certain Questions of Mutual Assistance in Criminal Matters (Djibouti/France),* Judgment of 4 June 2008, ICJ Reports 2008, 177, para. 135.

242 Convention on Cybercrime 2001 (n. 215), art. 27.

of a requested state and mutual trust between state parties. Such mutual trust may be difficult to achieve in cyberspace.[243] The statement of Russian president Putin with regard to request extradition of cybercriminals stands emblematically for the limits of mutual legal assistance when political will and mutual trust are missing:

> 'Russia will naturally [extradite] but only if the other side, in this case the United States, agrees to the same and will also extradite corresponding criminals to the Russian Federation.'[244]

The variety of recognized broad reasons for rejecting requests puts into question whether a minimum standard of cooperation can be assumed. One may however enquire whether states at least need to give reasons for refusing a request. In the ICJ case *Djibouti vs France* France was for example held accountable for failing to give reasons for its refusal of a mutual legal assistance request.[245] The duty to give reasons for a refusal to cooperate in criminal proceedings has also been acknowledged in international human rights law by the ECtHR.[246] Also the principle of good faith which is stipulated by Art. 4 of the ILC Draft Prevention Articles weighs in favour of assuming a duty to at least give reasons for refusing a cooperation request.[247]

Assuming such a duty would heighten the argumentative burden of uncooperative states. A duty to give reasons for rejecting cooperation may also incentivize states to establish responsible entities for international requests.[248] In particular, with regard to highly harmful cyber operations, refusals to cooperate may be hard to justify. Thus, it can be assumed that responding to and giving reasons for refusals of an assistance request are a binding minimum requirement.

---

243 De Busser, 'Recommendation 13d' 2017 (n. 119), para. 32.

244 Olga Pavlova, 'Putin says Russia prepared to extradite cyber criminals to US on reciprocal basis', *CNN,* 13 June 2021, available at: https://edition.cnn.com/2021/06/13/europe/putin-russia-cyber-criminals-intl/index.html.

245 ICJ, 'Mutual Legal Assistance in Criminal Matters' (n. 241), para. 156.

246 ECtHR, *Case of Güzelyurtlu and Others v. Cyprus and Turkey*, Grand Chamber Judgment of 29 January 2019, Application no. 36925/07, para, 266.

247 ILC Draft Articles on Prevention 2001 (n. 31), art. 4: 'States concerned shall cooperate in good faith (…)'; In the *Djibouti/France* case Djibouti argued that the lack of reasons provided by France regarding its refusal to cooperate violated good faith, see ICJ, 'Mutual Legal Assistance in Criminal Matters' (n. 241), para. 135.

248 On the importance of establishing points of contact for cybercrime prosecution see below chapter 4.D.IV.

4.3 Informal cooperation

Mutual legal assistance is often perceived as too slow and ineffective.[249] As a consequence, states have partially resorted to informal procedures, such as agency-agency cooperation, or direct contact between law-enforcement authorities, at times facilitated by an international agency, such as INTERPOL.[250] Informal cooperation can facilitate and accelerate formal cooperation[251] but it is so far under-utilized. There are several 'success' stories of informal cooperation. Yet, most states do not have a clearly prescribed set of rules for informal cooperation.[252] Informal cooperation hence lacks a sufficient level of coherency to inform a minimum or best practice due diligence standard. Furthermore, informal cooperation bears the risk of watering down procedural safeguards, in particular due process rights.

5. The challenge of assessing cybercrime cooperation standards beyond a minimum standard

Due to diverging standards in international practice and a complex web of international standards, a uniform due diligence standard of cooperation on cybercrime prosecution cannot be presumed. The UN GGE Reports and the wide net of formal and non-binding norms on cooperation regarding cybercrime however regularly create the normative presumption that states cooperate in good faith on cybercrime prosecution. As a bottom line states are required to give reasons for rejecting formal cooperation requests. To avoid the risk that cooperation is only fragmentary or limited to regional hubs, states are well advised to improve mutual legal assistance agreements

249 T-CY Cybercrime Convention Committee, T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime T-CY(2013)17rev (Provisional), Strasbourg, France 3 December 2014 T-CY assessment report: p. 123: 'Response times to requests of six to 24 months appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the positive obligation of governments to protect society', See also Anna Maria Osula, 'Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data', *Masaryk University Journal of Law and Technology* 9 (2015), 43–64, at 51.

250 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 209; see also Berkes, 'Human Rights in Cyberspace' 2019 (n. 62), 226.

251 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 209.

252 Ibid., p. 210.

and procedures. The Second Additional Protocol to the Budapest Convention may contribute to this aim.[253] Focusing on the improvement of such formalized procedures via specialized legal rules as *lex specialis* seems eventually more promising than resorting to an open-ended and largely undefined due diligence duty of cybercrime cooperation. In this regard the reluctance of the UN GGE Reports regarding general assertions on cybercrime cooperation requirements may be well reasoned.

V. Risk mitigation measures regarding ICT vulnerabilities

Vulnerabilities are a persistent problem for the security of ICT. Vulnerabilities are weaknesses or errors in the code, design or internal controls that enable the compromising of the CIA of ICT.[254] A vulnerability creates an entry point or an 'attack surface' for potential attackers if they have a tool or a technique to exploit the error.[255] The cross-cutting relevance of ICT vulnerabilities and its link to the integrity of the ICT supply chain[256] raises the question whether the obligation to exercise due diligence for harm prevention requires risk mitigation measures regarding ICT vulnerabilities. ICT vulnerability risk mitigation bundles both negative and positive obligations and with regard to the latter sits at the interface of procedural and institutional due diligence measures. It is discussed here in the context of procedural due diligence measures due to the importance of procedural rules for vulnerability disclosure processes, as well as due to links to other procedural due diligence measures, such as duties to notify or to assist.

253 Council of Europe, Second Additional Protocol **2021 (n.** 145**).** On the necessity of such a protocol, e.g. with regard to more effective procedures and more transparency see Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 March 2019, the UNODC/CCPCJ/EG.4/2019/2, 12 April 2019, paras. 16, 17.

254 In this vein National Institute of Standards and Technology, Glossary, vulnerability.

255 See UN GGE Report 2021, para. 11: 'New and emerging technologies are expanding development opportunities. Yet, their ever-evolving properties and characteristics also expand the attack surface, creating new vectors and vulnerabilities that can be exploited for malicious ICT activity.'

256 UN GGE 2015, para. 13i.

1. Definition of ICT vulnerabilities

The European Union Agency for Cybersecurity (ENISA) defines a vulnerability as

> '[t]he existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event (…) compromising the security of the computer system, network, application, or protocol involved'.[257]

Due to the complexity of programming and designing IT software and IT hardware, as well as time pressure in a competitive market[258], ICT products used by governmental agencies, critical infrastructures and private users inevitably have 'vulnerabilities'.[259] They are embedded in the design of ICT. The more vulnerabilities in IT products exist, the more surface attackers have to attack. As a consequence, wide-spread vulnerabilities risk to undermine the confidence in the global internet[260] and to adversely affect the global culture of cybersecurity. Reduction of vulnerabilities in ICT is hence a central prerequisite for a more resilient cyberspace.[261]

257 ENISA, Glossary, available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary.

258 Thomas Holt, 'What are software vulnerabilities, and why are there so many of them?', *The Conversation*, 23 May 2017, available at: https://theconversation.com/what-are-software-vulnerabilities-and-why-are-there-so-many-of-them-77930.

259 Klaus Lenssen, '…on the Ground: An Industry Perspective', in Ingolf Pernice/Jörg Pohle (eds.), *Privacy and Cyber Security on the Books and on the Ground* (Alexander von Humboldt Institute for Internet and Society 2018), 107–110, 110: 'We must acknowledge and (frustratingly) accept that software, hardware, and services vulnerabilities exist today and will continue to be discovered, no matter how hard we all work to avoid them. With millions of lines of code plus thousands of configuration options, and the ability of a single wrong keystroke to result in a bug that is not detected, complexity is quite possibly the single biggest contributing factor'; see also Lahmann Unilateral Remedies' 2020 (n. 146), 17.

260 Myriam Dunn Cavelty/Jacqueline Eggenschwiler, 'Behavioral Norms in Cyberspace', *The Security Times,* February 2019, p. 35; Lenssen, 'Industry Perspective' 2018 (n. 259), 109.

261 One of the central aims of the EU Cybersecurity Act is the identification of ICT vulnerabilities, see EU Regulation 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act), e.g. Rc. 30, art. 51d, g, j.

2. Exploitation of ICT vulnerabilities by intelligence and law enforcement

From the outset, the issue of ICT vulnerabilities is complicated by the fact that vulnerabilities, also termed 'zero-day exploits'[262], are not only exploited by cyber criminals but also exploited by law enforcement and intelligence services, for example to gather information in investigations or to potentially manipulate the operation of an IT system or network for law enforcement purposes. Hence, states often have an interest in retaining vulnerabilities they have found or bought.[263] The development, sale and distribution of hacking tools is a prolific business. The so-called *Pegasus* disclosures have revealed the widespread sale of the *Pegasus* spyware from the Israeli IT security firm NSO to various governments which in many cases subsequently targeted numerous journalists, human rights activists and politicians.[264] As most such transactions remain clandestine it is not possible to properly assess the number of sales of cyber 'weapons' to governments but disclosures of hackers trading with governments indicate that the number is significant.[265] Hence, it can be assumed that the question of vulnerabilities disclosure is a sensitive matter for the vast majority of states.

Purchasing and retaining a vulnerability is risky. Vulnerabilities may be discovered simultaneously by other malicious actors: According to security researchers between 10–20 % of vulnerabilities get discovered parallelly.[266] Furthermore, retained vulnerabilities may themselves be compromised, leaked or stolen. Before the *WannaCry* attack in 2017 the NSA for example stockpiled a vulnerability in a Microsoft software over years. The vulnerability was subsequently leaked to the group *Shadow Brokers*. After discovering the leak, the NSA disclosed the vulnerability to Microsoft which

262 Kellen Browning, 'Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack', *New York Times,* 2 July 2021, available at:https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html : 'a previously unknown vulnerability in its systems — known as a "zero day" (…) when such vulnerabilities are discovered, software makers have zero days to fix it'.

263 Thomas Wischmeyer, *Informationssicherheit* (Tübingen: Mohr Siebeck 2023), 282.

264 'Revealed: leak uncovers global abuse of cyber-surveillance weapon', *Guardian*, 18 July 2021, available at: https://www.theguardian.com/news/series/pegasus-project.

265 Eleonora Viganò/Michele Loi/Emad Yaghmaei, 'Cybersecurity of Critical Infrastructure', in Markus Christen Bert Gordijn Michele Loi (eds.) *The Ethics of Cybersecurity* (Berlin: Springer Natur 2020), 157–178, at 173, 174.

266 Bruce Schneier, 'Simultaneous Discovery of Vulnerabilities', *Schneier on Security*, 15 February 2016, available at: https://www.schneier.com/blog/archives/2016/02/simultaneous_di.html.

immediately issued a patch in March 2017. Yet, in May 2017 many users had not yet installed the patch and were hence vulnerable to the exploitation of the leaked vulnerability. The ensuing *WannaCry* attack caused massive economic damage and disruptions worldwide. Even some hospitals were partially shut down[267], exemplarily highlighting the risks of retaining vulnerabilities. It raises the question if and under which circumstances due diligence requires states to disclose ICT vulnerabilities they are aware of.

3. Vulnerability disclosure as a due diligence requirement

It has been argued that vulnerability disclosure falls outside of the realm of due diligence from the outset because in case of non-disclosure of a vulnerability by a state it cannot be said that the harmful cyber operation was emanating from that state's territory.[268] However, knowledge of a vulnerability will usually be gained by a state on its territory or under its control. Even if the acquisition of knowledge is not tantamount to control over the harmful actor who is exploiting the vulnerability and may operate on the territory of another state, a state is at least in the position to influence whether a vulnerability can be exploited by this third actor. Hence, it seems justified to assume due diligence-based accountability due to the knowledge-based capacity to influence the harmful act or its effects.[269] Grasping the issue of vulnerabilities disclosure under the due diligence rationale should therefore not be discarded from the outset. The issue of vulnerability disclosure is addressed in para. 13 lit. j of the UN GGE Report 2015 which asserts that:

> 'States should encourage responsible reporting of ICT vulnerabilities and share information on available remedies to such vulnerabilities to limit and possible eliminate potential threats to ICTs and ICT-dependent infrastructure'.

The text of para. 13 lit. j hence concerns two different aspects regarding vulnerabilities: On the one hand, the encouragement of the reporting of a vulnerability and on the other hand, the sharing of information on

267 Russell Brandom, 'UK Hospitals Hit with Massive Ransomware Attack', *The Verge,* 12 May 2017, available at: https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin.

268 Delerue, 'Cyber Operations' 2020 (n. 47), 373.

269 On capacity to influence as the underlying rationale of due diligence-based accountability chapter 2.A.III.

remedies. The text of the norm does not directly address vulnerability disclosure between states.

3.1 Reporting of ICT vulnerabilities

Regarding the regulation of responsible reporting, the text indicates that para. 13 lit. j is primarily conceived within the territory of a state and concerns reporting of discovered vulnerabilities by private actors to vendors. This corresponds to the classical understanding of vulnerability disclosure which circumscribes the process in which the finder informs the vendor (and not other states) of a vulnerability.[270] Para. 13 lit. j stipulates that states 'should encourage responsible reporting' – a normative aim that is also highlighted by the Paris Call of 2018.[271] *Adamson* has referred to the adoption of appropriate legislation as a potential measure.[272] More broadly, Canada has hinted at establishing 'national structures' to encourage reporting[273], similar to the UN GGE Report 2021 which argued for 'impartial legal frameworks, policies and programmes to guide decision-making on the handling of ICT vulnerabilities and curb their commercial distribution'.[274] To encourage reporting of vulnerabilities it is important to provide more legal certainty to 'white-hat' security researchers that they will not be subjected to investigation and prosecution following disclosure of a found vulnerability – an issue which the EU, as well as the UN GGE Report, has highlighted.[275] Too often, benevolent hackers who follow procedures to test the security of ICT products are subject to criminal investigations

270 See the definition under ISO/IEC 29147: 'Vulnerability disclosure is a process through which vendors and vulnerability finders may work cooperatively in finding solutions that reduce the risks associated with a vulnerability.'

271 Paris Call for Trust and Security in Cyberspace, 12 November 2018, p. 2: 'We recognize all actors can support a peaceful cyberspace by encouraging the responsible and coordinated disclosure of vulnerabilities.'

272 Adamson, 'Recommendation 13c' 2017 (n. 29), p. 74, para. 39.

273 Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, UN General Assembly A/75/816, 18 March 2021, Annex to the Chairs summary, Canada, p. 15.

274 UN GGE Report 2021, para. 62.

275 UN GGE Report 2021, para. 62: 'States could also consider putting in place legal protections for researchers and penetration testers.'; EU, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, (NIS 2 Directive),

after disclosing an identified ICT vulnerability. As the precise legislative measures for protecting security researchers are not further specified by states and as the UN GGE Report 2021 only hortatorily refers to the option to consider such measures[276], so far, putting such protections in place can however only be considered best practice.

The degree as to which a state decides to encourage reporting domestically affects the legally protected interests of other states only indirectly. This raises the question to what extent encouragement of reporting can be conceived as a best practice standard under the harm prevention rule.

Some states and commentators view the reporting of vulnerabilities as an obligation on the inter-state level. The text of para. 13 lit. j UN GGE Report 2015 does not indicate this but *Tsagourias* has directly deduced a duty to warn other states about vulnerabilities via a systematic reading of para. 13 lit. j in the light of the due diligence rationale expressed by para. 13 lit. c.[277] States' statements support the reading that international law vulnerability disclosure also applies between states. China, for example, considers reporting of vulnerabilities between states a CBM.[278] Canada referred to cooperation between national CERTs and hence to inter-state cooperation mechanisms to implement para. 13 lit. j of the UN GGE Report.[279] Also the UN GGE presupposes that vulnerability disclosure occurs between countries and national CERTs.[280] Due to the interest of every single state to acquire knowledge about ICT vulnerabilities such a conception of vulnerability disclosure as an inter-state obligation seems reasonable.

Rc. 60: '(…) Member States should aim to address (…) the challenges faced by vulnerability researchers, including their potential exposure to criminal liability(…).'

276 UN GGE Report 2021, para. 62.

277 Tsagourias, 'Recommendation 13j' 2017 (n. 200), para. 36: 'It can thus be contended that, to the extent that a general duty to inform, notify or warn exists in international law, it translates into a duty to inform other states of vulnerabilities that may cause damage to their infrastructure.'

278 China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 2020, p. 7, at V.

279 Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, UN General Assembly A/75/816, 18 March 2021, Annex to the Chairs summary, Canada, p. 11.

280 UN GGE Report 2021, para. 61: 'A coordinated vulnerability disclosure process can minimize the harm to society posed by vulnerable products and systematize the reporting of ICT vulnerabilities and requests for assistance between countries and emergency response teams'.

There are hence strong reasons to assume that the normative expectations to disclose vulnerabilities in principle also apply between states under the harm prevention rule. However, as China's categorization of vulnerability as a mere CBM indicates, a duty to warn about ICT vulnerabilities can, so far, only be considered an emergent norm, but not a binding due diligence requirement.

There is furthermore not yet an approximate standard under which conditions vulnerabilities need to be disclosed. States have only begun to be more transparent about their decision-making.[281] The lack of transparency and defined processes around vulnerabilities equities processes (VEP) is a concern.[282] A VEP involves a careful balancing of interests in retaining a vulnerability against the risks of retaining it. The UK and several civil society organizations have argued that the presumption in such processes should be in favour of disclosure.[283] While the UN GGE Report 2021 stipulated various examples of best practices it notably fell short of endorsing a presumption in favour of disclosure.[284]

Due to the lack of clarity, as a way forward, an exchange of views about VEP and publication of VEPs, such as by UK, including relevant criteria in the process, may strengthen resilience as a CBM. Such informal guidelines may provide legal yardsticks for the balancing of conflicting interests. The UK VEP e.g. introduces operational necessity, risks of discovery by someone else, as well as possible remediation as criteria for deciding whether a vulnerability is disclosed or not.[285] In any case, the precise steps in the iterative process of disclosing and remedying vulnerabilities is complex and no international minimum standard of due diligence or an approximation of a best practice currently exists. Nevertheless, due diligence arguably requires that states at least put foreseeable and sufficiently detailed process-

281 UK, The Equities Process, 29 November 2018, available at: https://www.ncsc.gov.uk/blog-post/equities-process; see Sven Herpig/Ari Schwartz, 'The Future of Vulnerabilities Equities Processes Around the World', *Lawfare*, 4 January 2019, available at: https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world.

282 As pointed out in the UN OEWG Chairs Summary 2021 (n. 9), para. 7.

283 GCSC, 'Final Report' 2019 (n. 146), Norm 4: 'States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.'

284 UN GGE Report 2021, para. 61.

285 UK, The Equities Process 2018 (n. 281).

es in place, based on which they decide whether they retain or disclose vulnerabilities.

3.2 Information on remedies

Also with regard to the provision of remedies it is not clear whether such an obligation to provide remedies exists on the inter-state level or only in relation to the public. The NAM[286] and the UN OEWG Final Report[287] refer to notification of *users*. Such a reading would align with Art. 13 of the ILC Draft Articles on Prevention which stipulates a duty to inform the public about risky activities.[288] This inward dimension of the information requirement tentatively suggests that it should be conceived as a due diligence requirement under the duty to protect human rights but not under the harm prevention rule. Yet, once a state knows about remedies for vulnerabilities, it would be detrimental for international cyber stability if a state was entitled to withhold such information from other states. Furthermore, if, as is argued here, vulnerability disclosure is conceived as an interstate obligation, it is only logically consequent that also informationsharing on remedies – which is an essential part of vulnerability disclosure – is owed to other states.[289] The complexities of the iterative process of sharing information about remedies in any case make it impossible to ascertain an

286 NAM Working Paper for the Second Substantive Session of the Open-ended Working Group on developments in the Field of Information and Telecommunications in the Context of International Security (UN OEWG), p. 1: 'Member States should be urged to consider the exchange of information on ICTs related vulnerabilities and/or harmful hidden functions in ICT products and to notify users when significant vulnerabilities are identified.'

287 UN OEWG Chairs Summary 2021 (n. 9), para. 25: 'States also proposed further ensuring the integrity of the ICT supply chain, expressing concern over the creation of harmful hidden functions in ICT products, and the responsibility to notify users when significant vulnerabilities are identified.'

288 ILC Draft Articles on Prevention 2001 (n. 31), art. 13: 'States concerned shall, by such means as are appropriate, provide the public likely to be affected by an activity within the scope of the present articles with relevant information relating to that activity, the risk involved and the harm which might result and ascertain their views.'

289 Arguing that sharing of remedies is an interstate obligation see Tsagourias, 'Recommendation 13j' 2017 (n. 200), para. 36, 37: 'the sharing of information about remedies, this is an interstate obligation (…) More specifically, it particularises (…) recommendation (c) on due diligence (…)'. It should be noted that the doctrinal differentiation may not be practically relevant. As soon as the public in one state

international standard, not to speak of a binding international minimum standard.

4. Links of state exploitation to attacks on the integrity of the supply chain

A closely related issue is the issue of exploitation and disclosure of ICT vulnerabilities via so-called 'attacks on the integrity of the IT supply chain'. The supply chain describes efforts to improve cyber security of IT products. In contrast to the exploitation of discovered ICT vulnerabilities attacks on the supply chain deliberately create a vulnerability already in the ICT production process. They are thus often referred to as installing 'backdoors'.[290] The *SolarWinds* hack discovered in 2020, as well as the ransomware attack exploiting a vulnerability in a Kaseya software in July 2021[291], highlighted the increasing interest of malicious cyber actors in such attacks on the integrity of the supply chain. Experts have underlined that attacks on the supply chain are particularly hideous and dangerous as they not only exploit technical vulnerabilities but affect the trust between customers and businesses and trust in the patching cycle process which is essential to increase cyber resilience.[292] Due to suspicions that the decision-making on technical standards is used for enabling the insertion of 'backdoors', the allegedly merely technical process of standard-setting in international fora has repeatedly become severely contested.[293]

---

is informed about remedies, other states will regularly acquire knowledge of the remedies as well.

290 Kim Zetter, 'Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers', *VICE*, 25 March 2019, available at: https://www.vice.com/en/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers.

291 Kellen Browning, 'Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack', *New York Times,* 2 July 2021, available at:https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html.

292 Written Testimony of Brad Smith President, Microsoft Corporation Senate Select Committee on Intelligence Open Hearing on the SolarWinds Hack, 'Strengthening the Nation's Cybersecurity: Lessons and Steps Forward Following the Attack on SolarWinds' February 23, 2021, p. 14: '(…) supply chain attacks that put technology users at risk and undermine trust in the very processes designed to protect them are out of bounds for state actors.'

293 Dennis Broeders, *The Public Core of the Internet* (Amsterdam University Press 2015), 46: Those protocols may well be technical or logical in nature, but that does not make them immune to interests, politics and power (…) For every protocol

5. The protection of the integrity of the supply chain in the UN GGE Report 2015

Para. 13 lit. i of the UN GGE Report 2015 on the integrity of supply chain asserts that:

> 'States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions'[294]

As is typical for the norms of responsible state behaviour these normative aspirations are expressly voluntary and non-binding. The formulation of para. 13 lit. i which refers to 'reasonable steps to ensure' suggests that a potential obligation is primarily a positive protective obligation. This however masks that the undermining of the supply chain is regularly incentivized from the state level and that therefore an obligation regarding this matter is a primarily negative one – not to undermine the integrity of the ICT by creating or pushing to create backdoors. This primarily negative dimension can be seen in the recommendations made by Microsoft regarding the protection of the IT integrity chain – all of which address state actors.[295] Intrusive state action also underlies the discussion around negative duties of states not to impair the public core of the internet, inter alia by hampering with technical standards.[296] Discharging this negative prohibitive dimension of para. 13 lit. i merely requires to refrain from acts that adversely affect the integrity of the supply chain.

---

that has been promoted to the status of a standard, there were alternatives that did not succeed for one reason or another.' On the power relations underlying technical protocols and standards Julie E. Cohen, 'Cyberspace As/And Space', *Columbia Law Review* 107 (2007), 210–256, at 256: 'about the visibility and scale of the power relations manifested through technical protocols and standards'.

294 UN GGE Reports 2015, para. 13 lit.i.

295 Microsoft, 'Six Proposed Norms to Reduce Conflict in Cyberspace', 20 January 2015, available at: https://www.microsoft.com/security/blog/2015/01/20/six-proposed-norms/, e.g. para. 1: States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services. In more detail on states' duties to refrain from targeting ICT companies to install backdoors Caitriona Heinl, 'Recommendation para. 13i', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 223–239, at 237, para. 38.

296 See chapter 3.C.III.

With regard to protective 'reasonable steps to ensure' the integrity of the supply chain partnering with private industry is a central requirement in order to improve resilience.[297] This may require to hold vendors accountable to ensure security of their products, but may also include the protection of encryption, or compliance with IT security standards in public procurement.[298] A further measure to contribute to the integrity of the supply chain may be the criminalization of supply chain attacks as misuse of devices.[299] While strong reasons speak for criminalization of misuse as the required international minimum standard more *opinio iuris* would be required to elevate it to the level of a binding due diligence requirement.[300]

6. Emergence of best practice standards regarding ICT vulnerability disclosure

The overall picture regarding international law on vulnerability disclosure processes and remedies is hence murky – or in the words of Canada a 'diversity of views on the matter'[301] exist. The statements highlight an increasing awareness that vulnerability disclosure is important for a more secure cyberspace. Yet, it is so far largely unclear which institutional and procedural measures states need to adopt to address this issue and whether such measures are owed to other states, derive from the harm prevention rule, from the duty to protect under human rights law or from a self-standing duty. State practice and commentators however point to emerging best practice standards. While the evolving best practices are only *soft law* and not a binding due diligence requirement the ongoing dialogue and exchange of such practices and relevant criteria, e.g. as a CBM, may harden over time to more stringent normative commitments and contribute to clarifying normative expectations. In developing best practice templates,

297 Canada, Canada's implementation of the 2015 GGE norms 2019 (n. 166), p. 13.
298 Heinl, 'Recommendation 13i' 2017 (n. 295), para. 38.
299 Microsoft, International Cybersecurity Norms, p. 13: 'States should establish processes to identify the intelligence, law enforcement, and financial sanctions tools that can and should be used against governments and individuals who use or intend to use cyber weapons in violation of law or international norms.' On the connection between para. 13i, j and criminal prosecution Heinl, 'Recommendation 13i' 2017 (n. 295), para. 39; on criminalization of misuse of devices see below chapter 4.D.I.4.1.
300 See in more detail chapter 4.D.I.4.1.
301 Canada's comments on zero draft text, February 2021, p. 8.

states would also need to distinguish more clearly between the actors involved and associated normative expectations during various stages of the disclosure process, for example between vulnerability disclosures by researchers or intelligence officials to vendors, and vulnerability disclosure between different states, or processes through which patches against vulnerabilities are distributed. In any case, states' interests in exploitation of ICT vulnerabilities will continue to make the issue sensitive for states and states likely aim to preserve a certain leeway for continuing to exploit ICT vulnerabilities. At this point in time, disclosure of ICT vulnerabilities can hence not be considered a binding due diligence requirement.[302]

VI. Summary on procedural due diligence obligations

The preceding analysis has shown that several legal yardsticks regarding procedural due diligence obligations can be discerned. The normative aspiration of cooperation underlies all other procedural due diligence obligations but a general due diligence duty to cooperate as such provides insufficient normative direction. Specific cooperative due diligence obligations are more relevant in practice: Due diligence requires states to take action with regard to ongoing or imminent harmful cyber operations emanating from their territory. Due diligence arguably also requires states to warn or inform other states about risks of cyber harm emanating from their territory. It is however unclear under which circumstances such a duty is triggered and states are so far reluctant to commit to a duty to warn in cyberspace. Due diligence also requires that states cooperate in good faith for cybercrime prosecution. At the very minimum due diligence requires that states give reasons for a refusal to comply with cybercrime cooperation requests. It is plausible that rules for international cooperation on cybercrime prosecution are and will continue to be specified via binding and non-binding *lex specialis* norms, rather than via a broad due diligence standard. Lastly, there are strong reasons to assume that a due diligence duty to conduct a legally balanced VEP, as well as a duty to disclose vulnerabilities to the public and other states, is emerging. States however would need to be more forthcoming with regard to relevant legal criteria. It is so far not clear whether such a duty can be conceived under the harm prevention rule or as

302 Also rejecting the illegality under international law of non-disclosure of vulnerabilities Delerue, 'Cyber Operations' 2020 (n. 47), 373.

a self-standing duty, and furthermore if such a duty is primarily owed to the public, to other states, or to the international community.

D. Due Diligence Measures Regarding a State's Institutional Capacity

Procedural due diligence obligations often presuppose institutional safeguards. This invites to assess the second broad category of due diligence obligations: Measures with regard to a state's institutional capacity. This category may include legislative and administrative safeguard measures.[303]

I. Cybercrime legislation and prosecution

A legislative measure of extraordinary importance is the criminalization of malicious behaviour in cyberspace. Prosecuting cybercrime is a key tool to reduce cyber instability. As noted by a UN Study on Cybercrime in 2013:

> '[C]riminalization gaps in any country can create offender havens with the potential to affect other countries globally'.[304]

Due to the principle of *nullum crimen sine lege* lack of legislation on cybercrime is an impediment to prosecution of cybercrime. If a country does not enact cybercrime legislation it cannot prosecute crimes committed via ICT. Due to the dual criminality rule[305], lack of cybercrime legislation is also permanently hindering securing evidence in criminal procedures, apprehension and extradition.[306] Even when foreign countries detect the actor behind malicious cyber activities they are prevented from requesting assistance or extradition if the territorial state has no similar criminal law in place. In the case of the ILOVEYOU virus in the Philippines in 2000 the perpetrator for example was known but could not be prosecuted as no legislation on cybercrime existed at the time in the Philippines.[307] Countries in which no cybercrime legislation exists are hence an ideal safe haven[308]

303 On categories of due diligence obligations see chapter 4.B.V.
304 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 77.
305 Ibid., p. 60; the AU Convention on Cyber security explicitly refers to the double criminality rule in art. 28 (1).
306 Clough, 'Challenges of Harmonisation' 2015 (n. 211), 701, 715.
307 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 14), commentary to rule 13, p. 77, fn. 104.
308 Clough, 'Challenges of Harmonisation' 2015 (n. 211), 701.

for cyber criminals. Such cyber safe havens affect the stability of cyberspace globally.[309] Due to importance of cybercrime legislation the question arises whether due diligence may require states to enact cybercrime legislation as a measure of institutional capacity-building, and if so, which legislative measures are required.

1. Criminal legislation and prosecution as due diligence requirements

The interrelation between criminal prosecution and due diligence was highlighted by early cases on due diligence in which states were held responsible for exercising due diligence in investigating and apprehending non-state actors for injuries to aliens. In the *Janes* case the Tribunal held the Mexican government responsible for violating its 'duty of diligently prosecuting and properly punishing the offender'.[310] In the *Lotus* case, *Judge Moore* asserted:

> '[I]t is well settled that a State is bound to use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people'[311]

In the ICJ *Corfu Channel* case Judge Alvarez linked the enactment of substantive criminal law provisions to due diligence for harm prevention, referring to the necessity to criminalize acts 'to the detriment of other states or of their nationals'.[312] As asserted in the *Janes* case not only criminalization is required but also effective prosecution – or put differently in the

309 The necessity of cybercrime legislation was already underlined in UN General Assembly Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, UN General Assembly A/75/816, 18 March 2021, Annex to the Chairs summary A/RES/55/63, 22 January 2001, para. 1: 'Notes with appreciation the efforts of the above-mentioned bodies to prevent the criminal misuse of information technologies, and also notes the value of, inter alia, the following measures to combat such misuse: (a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies (…)'.

310 *General Claims Commission (Mexico-USA), Janes*, 16 November 1925, UNRIAA, vol. IV, 87.

311 PCIJ, *The Case of the S.S. Lotus (France v. Turkey)*, Dissenting Opinion by Moore, 7 September 1927, Series A, No. 10, 88.

312 ICJ, *Corfu Channel Case (United Kingdom v. Albania)*, Separate Opinion of Judge Alvarez, ICJ Reports 1949, 4, p. 44, para. 4.

words of the ICJ in *Pulp Mills* due diligence requires 'not only the adoption of appropriate rules and measures, but also a certain level of vigilance in their enforcement'.[313]

While the Tallinn Manual negated that enacting cybercrime legislation under the harm prevention rule was required in cyberspace, due to its restrictive stance on due diligence requirements[314], several states, such as Canada or the UK, have linked enactment of cybercrime legislation to the harm prevention rule.[315] In a thinly veiled reference to the due diligence rationale regarding criminal activities emanating from Russian territory the US has argued that:

> '[O]ur view is that when there are criminal entities within a country, [the country] certainly ha[s] a responsibility and it is a role that the government can play'[316]

Although the statement did not explicitly mention cybercrime legislation it is aimed at criminal prosecution which requires such legislation. This indicates that states increasingly recognize that the requirement to enact criminalization and to prosecute harmful actors is required to discharge due diligence in cyberspace.

2. Criminal legislation and prosecution under international human rights law

Also the due diligence duty to protect in human rights law may require criminal legislation and effective prosecution.[317] Effective criminal prosecution, particularly for interferences with the right to life, is stressed in the

313 ICJ, 'Pulp Mills' (n. 111), para. 197.

314 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 22), commentary to rule 7, p. 45; see also Woltag, 'Cyber Warfare' 2014 (n. 212), 101.

315 Canada's implementation of the 2015 GGE norms 2019 (n. 166), p. 4; UK, 'Efforts to Implement Norms' 2019 (n. 87), p. 6; also arguing for cybercrime legislation to discharge the duty to exercise due diligence Adamson, 'Recommendation 13c' 2017 (n. 29), p. 73, para. 36.

316 Maegan Vazquez/Allie Malloy, 'Biden will discuss recent cyber attack on meat producer with Putin in Geneva', *CNN*, 2 June 2021, available at: https://edition.cnn.com/2021/06/02/politics/biden-putin-jbs-foods-russia/index.html.

317 Krešimir Kamber, 'Substantive and Procedural Criminal Law Protection of Human Rights in the Law of the European Convention on Human Rights', *Human Rights Law Review* 20 (2020), 75–100, at 75.

jurisprudence of the ECtHR[318] and the Inter-American Court of Human Rights (IACtHR)[319], as well as by the UN Human Rights Committee.[320] Regarding the cyber context, the ECtHR affirmed the necessity of cybercrime legislation for the protection of the right privacy in the *KU/Finland* case in 2008:

> '[The] obligations [to protect] may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves (…) While the choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is, in principle, within the State's margin of appreciation, effective deterrence against grave acts, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions'[321]

Also in the *Bărbulescu* case – which concerned cyber-enabled privacy intrusions against an employee by an employer – the ECtHR reaffirmed that a state may discharge its due diligence duties to protect human rights against cyber threats via criminal legislation.[322] Regarding criminalization, due diligence requirements under the duty to protect human rights hereby concur with due diligence requirements for harm prevention.

318 ECtHR, *Case of Nikolova and Velichkova v. Bulgaria*, Judgment of 20 December 2007, Application No. 7888/03, para. 57; ECtHR, *Case of Kilic v. Turkey,* Judgment of 28 March 2000, Application no. 22492/93, paras. 62, 63; see also Baade, 'The Duty to Protect' 2020 (n. 64), 94.

319 IACtHR, *Case of Velásquez-Rodríguez v. Honduras*, Judgment of 29 July 1988, Series C No. 4, para. 174.

320 UN Human Rights Committee, General Comment No. 36 on article 6 of the International Covenant on Civil and Political Rights, on the right to life, 30 October 2018, CCPR/C/GC/36, para. 21: 'States parties must further take adequate measures of protection, (…) in order to prevent, investigate, punish and remedy arbitrary deprivation of life by private entities.'

321 ECtHR, *Case of K.U. v Finland*, Judgment of 2 December 2008, Application no. 2872/02, paras. 43, 46.

322 ECtHR, *Case of Bărbulescu v Romania*, Grand Chamber Judgment of 5 September 2017, Application no. 61496/08, paras, 115, 116.

3. Assessing international standard on cybercrime legislation and prosecution

This raises the question whether a least common denominator regarding criminalization of cybercrime can be presumed. So far no global cybercrime treaty exists. It also seems uncertain whether a global multilateral treaty on cybercrime will be concluded in the foreseeable future. After more than two years of contested negotiations an intergovernmental committee, established by the UN General Assembly to work on an international convention on cybercrime, could not agree on a draft text for an international convention' on cybercrime in its concluding session in February 2024.[323]

Yet, a number of regional cybercrime conventions are relevant for determining international standards on criminalization. Conduct under treaty law counts as state practice.[324] As the customary standard of diligence needs to be interpreted systematically within the context of other rules of international law[325] this state practice also influences the interpretation of due diligence under the harm prevention rule.

Of particular relevance is the Budapest Convention of the CoE.[326] The convention has been pitched as the international 'benchmark' and guideline for attempts to harmonize criminal law provisions.[327] Beyond the Budapest Convention, the 2014 *Malabo* Convention on Cybersecurity and

323 From the outset, it had been disputed whether a global convention on cybercrime is feasible or even desirable. Already the vote in the UN General Assembly on the Russian proposal to establish an intergovernmental committee was severely contested (79 to 60, 33 abstentions, 21 non-voting), UN General Assembly Resolution A/RES/74/247, 27 December 2019.

324 ILC, Draft conclusions on identification of customary international law, UN A/73/10, conclusion 6 (2): 'Forms of State practice include (…) conduct in connection with treaties; executive conduct, including operational conduct "on the ground"; legislative and administrative acts (…).'

325 On the need to interpret due diligence systemically within the context of other rules of international see above chapter 4.B.III.

326 Convention on Cybercrime 2001 (n. 215).

327 See already Marco Gercke, 'The Slow Wake of A Global Approach Against Cybercrime', *Computer Law Review International* 5 (2006), 140–145; see also Report of the Chairman of HLEG, ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG) to ITU Secretary-General, Dr. Hamadoun I. Touré by Chief Judge Stein Schjølberg, p. 6,7, para. 1.3, para. 1.4.: '. It is very important to implement at least Articles 2–9 in the substantive criminal law section, and to establish the procedural tools necessary to investigate and prosecute such crimes as described in Articles 14–22 in the section on procedural law.'

Data Protection of the AU[328], the Convention on Combating Information Technology Offences of 2010 of the Arab League[329], and the 2009 SCO Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security are further relevant regional cybercrime treaties.[330] The EU Directive 2013/40 'establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems'.[331] This variety of regional instruments[332] on cybercrime shows that cybercrime is the one area of international law in which states so far have been more forthcoming in committing to binding rules. Tellingly, the offences of the cybercrime treaties do not apply to state-sponsored activities[333], hence, committing to binding rules is less costly for states as their own cyber activities remain uninhibited.

3.1 Criminalization requirements under cybercrime treaties

Regarding the substantive requirements stipulated in the convention it is important to note that the various conventions do not only address core-cyber harm offences against the confidentiality, integrity and availability of ICT systems and networks, but also include provisions on computer-related offences, such as forgery and fraud, or content offences, such as xenophobia, child pornography, terrorist propaganda.[334] The following analysis

328 African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), 27 June 2014. The Convention entered into force in June 2023 after its 15th ratification.

329 Arab Convention (n. 228).

330 SCO Agreement International Information Security 2009 (n. 123).

331 EU, 2013/40 of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA Directive.

332 See also the model cybercrime laws by the Caribbean Community (CARICOM), Model Legislative Texts of Cybercrime/e-Crimes and Electronic Evidence Model legislation targeting the prevention and investigation of computer and network related crime Non-binding Commonwealth – Model Law on Computer and Computer Related Crimes, available at: https://www.unidir.org/cpp/en/multilateral-frameworks.

333 Lahmann, 'Unilateral Remedies' 2020 (n. 146), 20.

334 Convention on Cybercrime 2001 (n. 215), arts. 7–10; Arab Convention (n. 228), arts. 10–18; the AU Convention also entails provisions on data protection, see Malabo Convention (n. 328), art. 8f.

will exclude these offences from the analysis due to this study's exclusive focus on cyber harm.[335]

With regard to offences which cause cyber harm, i.e. offences that compromise the confidentiality, integrity and availability of ICT, a converging minimum standard as the bottom line has emerged. Nevertheless, states have a certain degree of flexibility to implement this minimum standard as no uniform standard can be detected.

To begin with, all regional conventions require criminalization of access operations.[336] Art. 2 of the Budapest Convention exemplarily requires:

> 'Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. (…)'[337]

The other conventions entail similar provisions on access operations.[338] Deviations exists with regard to details. In order to avoid over-criminalization the EU Directive for example excludes 'minor cases' and furthermore requires an 'infringement of a security measure'.[339] An important *de minimis* threshold for criminalization may also be the exemption of security researchers.[340] Further deviations exist with regard to aggravating circumstances. The EU Directives 2013/40 for example stipulates operations against the information systems of critical infrastructure as an aggravating circumstance.[341]

Despite such divergences as to the specific criminalization access operations are almost universally criminalized. Already in 2013 the UN Study

335 See on the concept of cyber harm of this study which excludes content harm chapter 1.B.III.

336 For a definition of access operations see UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 257: 'Refers to acts involving gaining access to computer data without authorization or justification (…) This is the case, for example, if a perpetrator illegally accesses a computer database (…) if a perpetrator, who is working for a particular company, copies files to take with him without authorization.

337 Convention on Cybercrime 2001 (n. 215), art. 2.

338 Arab Convention (n. 228), art. 6; Malabo Convention (n. 328), art. 29 (1a-c); EU Directive 2013/40 (n. 331), art. 3.

339 EU Directive 2013/40 (n. 331), art. 3. See also the Convention on Cybercrime 2001 (n. 215), art. 2: '(…) A Party may require that the offence be committed by infringing security measures (…)'.

340 On the importance of IT security researchers for the detection of ICT vulnerabilities see above chapter 4.C.V.4.1.

341 EU Directive 2013/40 (n. 331), art. 9 (4c).

found that only 7 % of surveyed states had not yet criminalized access operations.[342] This suggests that criminalizing access operations can be considered the international minimum standard. A state cannot argue that it acted diligent if it has not criminalized access operations.

Aside from access operations, also interception of communications between ICT users or generally of data in transfer can compromise the confidentiality of data exchange processes.[343] Interception may occur directly through computer systems or indirectly, e.g. through technical devices fixed to transmission lines, or through the use of software.[344] Attackers usually search for weak entry points regarding transmitted communication points, for instance wireless connections.[345] While access operations are primarily directed at stored data interception abuses the particular vulnerability of data in transmission. Interception is particularly relevant with regard to cloud storage, and email transmissions which are particularly vulnerable.[346]

All multilateral treaties entail provisions requiring criminalization of interception of computer data.[347] 95 % of states surveyed in the UN Comprehensive Study on Cybercrime in 2013 had criminalized interception of computer data in their domestic law. The largely homogeneous criminalization of interception is however not tantamount to a uniform international standard. States' legislation is for example structured differently. Some states have enacted a cyber-specific provision on interception, other have included it in a general offence.[348] Despite such divergences in details, criminalization of the interception of non-public transmissions of computer data can be considered the international standard and a state is negligent if interception of data transfer in cyberspace is not criminalized in its domestic law.

Further offences which cause cyber harm are data and system interference. Both are interrelated. If a cyber operation affects the integrity and availability of computer data, it constitutes data interference. As data is non-tangible, interference with data is frequently not covered by traditional

342 UN ODC, 'Comprehensive Study' 2013 (n. 214).
343 ITU, Understanding Cybercrime: Phenomena, Challenges and Legal Response (ITU: September 2012), p. 19.
344 See CoE, 'Explanatory Report' (n. 238), p. 10, para. 53.
345 ITU Understanding Cybercrime 2012 (n. 343), p. 20.
346 Ibid., p. 19.
347 Convention on Cybercrime 2001 (n. 215), art. 3; Arab Convention (n. 228), art. 7; Malabo Convention (n. 328), art. 29 (2a); EU Directive 2013/40 (n. 331), art. 6.
348 UN ODC, 'Comprehensive Study' 2013 (n. 214),p. 78.

criminal law provisions on damage to physical objects.[349] As data interference may impair the smooth operation of software or computer systems[350], it may thereby amount to system interference.[351] A means to interfere with computer data is e.g. ransomware which allows an offender to encrypt files and deny access to victims unless they pay a ransom to decrypt the files.[352] Also computer worms – replicating programs that can initiate data-transfer processes within a network – or DDoS operations, may interfere with computer data and computer systems.[353] The effects of data and system interference are often graver than access and interception offences as not only the confidentiality of data, but also its integrity and availability may be affected, leading to potentially disruptive or even destructive physical consequences.[354]

It is hence unsurprising that all cybercrime treaties require the criminalization of data and system interference.[355] Consequently, the overwhelming majority of states have enacted criminal legislation.[356] The regional norms slightly differ with regard to the necessity of harm, or damage as a consequence of data interference. Both the Budapest Convention and the EU Directive for example exclude criminalization of minor cases.[357] In several domestic legislations data and system interference are criminalized via a single offence.[358] Similar to criminalization of access and interception operations state practice is hence largely homogeneous, despite divergences on details. Furthermore, no state has taken an explicit or implicit stance

349 Ibid., p. 88.
350 Ibid.
351 For examples of system interference, e.g. operations against CNN, Amazon or eBay, with severe disruptive potential see ITU Understanding Cybercrime 2012 (n. 343), p. 20.
352 Ibid.
353 Ibid.
354 On different degrees of cyber harm see chapter I.C.
355 Convention on Cybercrime 2001 (n. 215), art. 4; Arab Convention (n. 228), art. 8; Malabo Convention (n. 328), arts. 29 (2b), (2d); EU Directive 2013/40 (n. 331), arts. 4, 5.
356 See e.g. Criminal Law of the People's Republic of China, arts. 285–287; US, Computer Fraud and Abuse Act, 18 United States Code 1030, 1986; Argentina, Cybercrime and Violation of Privacy Act, Law no. 26.388; German Criminal Code, sections 303a, 303b; see for further references Coco/Dias, 'Cyber Due Diligence Report' 2021 (n. 129), 215.
357 EU Directive 2013/40 (n. 331), art. 5: '(…) at least for cases which are not minor'; Convention on Cybercrime 2001 (n. 215), art. 4.
358 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 89.

against criminalization of data and system interference. In particular, no state has argued that a requirement would impede its sovereignty or that it would exceed its capacity. A state hence acts negligent if it does not criminalize data and system interference.

More difficult is the assessment of the development and sale of 'software tools' which exploit vulnerabilities or weaknesses in the design of ICT. Production, possession and distribution of such software tools is an increasingly profitable business.[359] In the context of cybercrime treaties, it is frequently framed as 'misuse of devices'.[360] The private Israeli company NSO is a prominent example of a company developing 'software tools' to exploit ICT vulnerabilities and selling them to interested state parties.[361]

International legal practice has increasingly pushed towards illegalizing such activities. Para. 13 lit. i of the UN GGE Report 2015 for example asserts:

> '(…) States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions'[362]

The Budapest Convention and the Arab League Convention require criminalization of 'misuse of devices'.[363] Already in 2013, the majority of countries surveyed in a UN study had criminalized the misuse of devices.[364] Yet, divergences exist as to whether possession, creation, distribution and use is generally criminalized or only some of these acts.[365] The conventions provide for exceptions to the requirement to criminalize. The Budapest Convention for example adds 'without right' as an additional requirement

359 See above chapter 4.C.V.

360 The UN Study refers to misuse of devices as 'development or distribution of hardware or software solutions that can be used to carry out computer or internet-related offences', see UN ODC, 'Comprehensive Study' 2013 (n. 214), Annex One: Act Descriptions, p. 257.

361 'Cyber-surveillance weapon' 2021 (n. 264); see also Mehul Srivastava, 'WhatsApp voice calls used to inject Israeli spyware on phones', *Financial Times*, 14 May 2019, available at: https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab.

362 UN GGE Report 2015, para. 13 lit. i.

363 Convention on Cybercrime 2001 (n. 215), art. 6; Arab Convention (n. 228), art. 8; Malabo Convention (n. 328), Art. 29 (1h); EU Directive 2013/40 (n. 331), art. 7.

364 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 81.

365 Ibid.

for criminalization[366], similar to Art. 7 of the EU/2013/40.[367] The Explanatory Notes clarify that this means that criminalization is not required when the activity is conducted for 'legitimate purposes'.[368] Arguably, 'legitimate purposes' could be law enforcement or intelligence purposes. In this reading, selling ICT 'weapons' to governments by a private company may be exempted from the criminalization requirement.[369] Further restrictions on criminalization exist. Some states e.g. only criminalize the production and distribution of software tools when the software is used to commit a crime or when it is exclusively designed to commit a crime.[370] This ambiguous picture regarding the criminalization of 'misuse of devices' is concerning: Software tools exploiting the vulnerability of ICT create cyber instability.[371] Selling software tools to authoritarian countries makes it all but certain that human rights safeguards for intercepting and surveilling will be disregarded[372], and may furthermore affect the integrity of the supply chain. While treaty norms, the majority of state practice and the normative aim of para. 13 lit. i of the UN GGE Report 2015[373] suggest that states should severely curtail exemptions to criminalization, state practice, so far, is not sufficiently consistent to assume that this is the required standard of due diligence.

366 UN ODC, 'Comprehensive Study' 2013 (n. 214), art. 6.

367 EU Directive 2013/40 (n. 331), art. 7: 'the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right (…)'.

368 CoE, 'Explanatory Report' (n. 238), paras. 76, 77.

369 The private Israeli firm NSO openly admits to selling 'spyware' and further hacking tools to governments, see 'Pegasus: Spyware sold to governments 'targets activists'', *BBC,* 19 July 2021, available at: https://www.bbc.com/news/technology-57881364.

370 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 257.

371 See above chapter 4.C.V.

372 The revelations around the so-called 'Pegasus'project are a case in point, see Cybersurveillance weapon' 2021 (n. 264).

373 UN GGE Report 2015, para. 13i: 'States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions'; in more detail see above chapter 4.C.V.7.

3.2 Convergence on an international minimum standard

Due to the convergence between the various regional treaties and state practice criminalization of access, interception operations and system and data interference it can be assumed that due diligence requires criminalization of such activities. Regarding the criminalization of misuse of devices states are more permissive and allow for various exemptions to criminalization. States are however at least required to generally criminalize the distribution and sale of vulnerability-exploiting software tools.

Assuming that due diligence requires criminalization of such activities is not tantamount to assuming a uniform international standard. Divergences exist with regard to details, such as *de minimis* exclusion, or systematic divergences within the structure of domestic criminal law. Also the specificities of a domestic criminal system, e.g. regarding intent, omission, attempt, negligence etc. preclude a uniform international standard.[374] It is hence clear that the international minimum standard does not require identical laws.[375] Criminalization however needs to ensure that the criminal legislation on these core cyber offence is not lax or inadequate.[376] Relegating criminalization of core cybercrime offences to mere voluntary guidelines would not give justice to the homogeneous state practice and the importance of eliminating cyber safe havens for global cyberspace.

4. Criminal procedural law as a due diligence requirement

Cybercrime legislation as such would largely lack teeth, if there would be no means to enforce it via criminal procedural law. In order for cybercrime legislation to have a deterrent effect with a preventive impact it is necessary to enact criminal procedural laws, and to implement them.[377]

The necessity of enacting criminal procedural legislation was already highlighted by a resolution of the UN General Assembly in 2000 which addressed the necessity of introducing procedural measures to address the problem of securing and accessing evidence in cybercrime matters, in particular electronic data. It stated that:

374 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 79.
375 Clough, 'Challenges of Harmonisation' 2015 (n. 211), 701.
376 See this formula in General Claims Commission, 'Janes' (n. 310).
377 GCSC, 'Final Report' 2019 (n. 146), p. 24.

> 'Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations'.[378]

The UN Comprehensive Study of 2020 asserted that it was 'imperative to develop adequate (…) data retention/data preservation rules'.[379] Scholars have assumed that due diligence requires the 'establishment of investigative cyber capabilities[380] and have linked due diligence to prosecution.[381] Also Canada has explicitly linked its enactment of cybercrime legislation and criminal procedural legislation regarding cyber offences to the harm prevention rule.[382]

4.1 Standard procedural measures

As data storage is costly, stored computer data is often stored only temporarily by internet service providers, at times only seconds, minutes, hours, days or weeks. Frequently, domestic legislation also requires the erasure of data by default immediately or after some period of time, inter alia for the protection of privacy.[383] In criminal investigations of cybercrime it is hence often problematic that some data is not accessible after a certain period of time.

Thus, in order to secure data for potential investigations, all agreements on cybercrime entail provisions on expedited preservation of computer data.[384] Accordingly, the vast majority of states has enacted legislation on

378 UN General Assembly Resolution A/RES/55/63, 22 January 2001, para. F.
379 UN Study, Draft Report, 29 July 2020, UNODC/CCPCJ/EG.4/2020/L.1/Add.1, para. 33.
380 Monnheimer, 'Due Diligence' 2021 (n. 36), 189.
381 Matthew Sklerov, 'Solving the Dilemma of State Response to Cyberattacks', *Military Law Review* 201 (2009), 1–85, at 13; Adamson, 'Recommendation 13c' 2017 (n. 29), p. 73, para. 36.
382 Canada's implementation of the 2015 GGE norms 2019 (n. 166), p. 4.
383 On the normative aim to save personal data for the shortest time possible, EU General Data Protection Regulation (EU) 2016/679 (GDPR), 27 April 2016, art. 5 (1e): 'Personal data shall be (…) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (…)'; Rc. 39.
384 Convention on Cybercrime 2001 (n. 215), art. 16; Arab Convention (n. 228), art. 23; Malabo Convention (n. 328), Art. 31 (3e).

expedited preservation of data.[385] Furthermore, the major cybercrime treaties require legalizing orders for computer data, hereby enabling that data is not only preserved but also obtained by law enforcement authorities.[386] All cybercrime treaties also require legalization of real-time collection of traffic data interception of content data.[387] While the vast majority of states has implemented legalizing such measures still a substantial amount has not yet done so, despite the 'fundamental' need to rely on such data in investigations.[388]

Nevertheless, state practice suggests that establishing legislation on four cyber investigative capabilities – preservation of data, order to obtain preserved data, interception of traffic and content data – can increasingly be considered the international standard. Yet, two aspects call into question whether it is promising to conceive the establishment of such capabilities as a due diligence requirement.

4.2 Divergences regarding human rights safeguards

With regard to criminal procedural it is important to point out that a uniform due diligence standard is unrealistic and even undesirable from the outset. A uniform standard regarding preservation of data risks leading to a race to the bottom for human rights safeguards in criminal procedural law. Already the preservation of data interferes with the right to privacy. Mindful of the risks of investigative capabilities for privacy the UN General Assembly Res. 68/167 on the right to privacy in the digital age required states to 'review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data' with a view to protecting privacy'.[389] Also the UN Human

385 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 128; see e.g. Jamaica, The Cybercrimes Act 2015, no. 31, section 14; Kenya, Computer Misuse and Cybercrimes Act 2018, sec. 51; US, 18 United States Code, Crimes and Criminal Procedure, § 2703(f).

386 UN ODC, 'Comprehensive Study' 2013 (n. 214), 122.

387 Convention on Cybercrime 2001 (n. 215), art. 20, 21; Arab Convention (n. 228), art. 29; Malabo Convention (n. 328), Art. 31 (3a-c).

388 UN ODC, 'Comprehensive Study' 2013 (n. 214), 128.

389 UN General Assembly, 'Right to privacy in the digital age' 2013 (n. 36), para. 4c: 'Calls upon all States (…) (c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a

Rights Council Res. 26/13 and the UN GGE Report 2021, as well as e.g. Canada[390], have highlighted that addressing security concerns and gathering of evidence in cyberspace needs to comply with international human rights law and other rules of international law generally.[391] The need to assess human rights-compliance of cyber investigative measures seems particularly acute as measures, such as data retention or interception, may also be applied beyond the cyber context with regard to general offences.[392] It is hence important to enact human rights safeguards regarding criminal procedural measures. Such safeguards could for example be restrictions of more intrusive measures, such as interception of content or traffic data, to graver crimes or to ensure judicial authorization or review of procedural measures, or to require due care in investigations.[393]

The extent to which states have implemented such human rights safeguards in state practice deviates. Art. 15 of the Budapest Convention requires 'adequate protection of human rights and liberties'.[394], By contrast, the Arab League Convention on Cybercrime concerningly does not include provisions on human rights safeguards. Also the Malabo Protocol contains only very little rules for criminal procedure and no human rights safe-

view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law.'

390 UN OEWG Chairs Summary 2021 (n. 273), Annex, Canada, p. 12.

391 UN GGE Report 2021, para. 33: '(…) States are also encouraged to develop appropriate protocols and procedures for collecting, handling and storing online evidence relevant to criminal and terrorist use of ICTs and provide assistance in investigations in a timely manner, ensuring that such actions are taken in accordance with a State's obligations under international law'; UN Human Rights Council, 'Human Rights on the Internet' 2014 (n. 63), para. 5: 'Calls upon all States to address security concerns on the Internet in accordance with their international human rights obligations to ensure protection of freedom of expression, freedom of association, privacy and other human rights online (…)'.

392 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 124. Draft art. 23 (2c) of the currently negotiated international convention on cybercrime e.g. requires states to apply its procedural measures for 'any criminal offence', UN GA, Revised draft text of the convention, A/AC.291/22/Rev.1, 6 November 2023, draft art. 23 (2c); highly critical regarding this aspect from the perspective of human rights Tomaso Falchetta, 'The Draft UN Cybercrime Treaty Is Overbroad and Falls Short On Human Rights Protection', *JustSecurity*, 22 January 2024, available at: https://www.justsecurity.org/91318/the-draft-un-cybercrime-treaty-is-overbroad-and-falls-short-on-human-rights-protection/.

393 Ibid., p. 134–136; Sven Herpig, *A Framework for Government Hacking in Criminal Investigations* (Stiftung Neue Verantwortung 2018), p. 21.

394 Convention on Cybercrime 2001 (n. 215), art. 15-.

guards.[395] The UN Study of 2013 noted that 15 % of countries replying to a questionnaire had no safeguards for protection of privacy, and human rights more generally, in place.[396] Due to the intrusiveness of some investigatory measures, such a lack of safeguards almost certainly leads to violations of human rights. Even within like-minded countries, such as the EU, divergences regarding procedural safeguards in criminal investigations exist.[397] Due to these divergences regarding human rights safeguards it seems futile to assume an international legal standard for investigative capabilities. Tellingly, the negotiations on an international convention on cybercrime reached a deadlock inter alia due to divergent positions on human rights safeguards and the principle of proportionality.[398] Even if states could agree on the principles of necessity, subsidiarity and proportionality regarding investigative measures, the margin of appreciation of implementing is so wide that it is also hard to point to an internationally recognizable best practice standard. Due to these wide divergences it should be cautioned against a uniform due diligence data preservation standard as such a standard may trigger an overzealous and human rights-violating implementation.

4.3 Diverging capacities

A further concern against assuming a binding due diligence standard for cyber investigative capabilities is the diverging technological capacity of states. The vast majority has indicated that it may require technical assistance in cybercrime prosecution.[399] Divergences in capacity were initially also a problem in Europe.[400] Some states face significant capacity problems

395 Malabo Convention (n. 328), art. 31 (3).
396 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 136.
397 De Busser, 'Recommendation 13d' 2017 (n. 119), para. 4: 'The significant difficulties (…) on the level of the EU when making efforts to harmonize substantive and procedural criminal law of the member states, demonstrate that this is an objective that should not be underestimated'. On the complexity of ECJ cases on data retention and collection with ramifications for cross-border data transfer see Christakis/Terpin, 'Law enforcement access to data' 2021 (n. 212), 25.
398 Alexis Steffaro, 'Detour or Deadlock? Decoding the Suspended UN Cybercrime Treaty Negotiations', 4 March 2024, available at: https://www.centerforcybersecuritypolicy.org/insights-and-research/detour-or-deadlock-decoding-the-suspended-un-cybercrime-treaty-negotiations.
399 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 178.
400 Clough, 'Challenges of Harmonisation' 2015 (n. 211), 725, fn. 252.

or have insufficient technology.[401] As a result, technologically less developed states may shy away from signing the Budapest Convention because they are unable to comply with the procedural requirements, e.g. on interception of traffic or content data.[402] The slow ratification of the AU Malabo Protocol may, inter alia, have been due to concerns over insurmountable capacity limits.[403]

Instead of asserting uniform due diligence standard on investigative capabilities it seems hence more worthwhile to focus on capacity-building and technical assistance[404], for example through training 'sufficient training of investigators, prosecutors and judges'.[405] Several states underlined that capacity-building is crucial to foster international cooperation for cybercrime prosecution in the ongoing UN Comprehensive Study.[406]

4.4. The gradual emergence of an international minimum standard and associated risks

The establishment of investigative cyber measures on data preservation, ordering of data and interception can increasingly be considered the predominant international standard. Due to diverging capacities it can however so far not be considered a binding due diligence requirement. Framing the establishment of investigative cyber capabilities as a binding due diligence requirement may furthermore prove counterproductive: It risks to incentivize the excessive extension of investigative capabilities which disregard the requirements of necessity, subsidiarity and proportionality under international human rights law.

401 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 123, 152, 172.
402 Clough, 'Challenges of Harmonisation' 2015 (n. 211), 725.
403 Ibid.
404 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 178.
405 Expert Group Report 2019 (n. 253), p. 3, para. 10 lit.b: '(…) other Member States suggested that it was not necessary or appropriate to consider a new global legal instrument because the challenges posed in respect of cybercrime and the sufficient training of investigators, prosecutors and judges were best addressed through capacity-building, active dialogue and cooperation among law enforcement agencies (…)'.
406 Ibid.

II. Level of actual or constructive knowledge under the harm prevention rule

In order to hold a state accountable under the due diligence standard it is necessary that the state had knowledge of the harmful activity.[407] Yet, when is a state expected to have known, or in the words of ICJ Judge Alvarez in *Corfu Channel* – when does a state have a 'duty to have known'[408] in cyberspace? Which proactive steps of institutional capacity-building does due diligence require from states to acquire knowledge?

1. No rebuttable presumption of knowledge

The mere fact that a cyber operation is emanating from a state's territory neither implies that the state knew or that it ought to have known of it, nor creates a rebuttable presumption that it knew. As the ICJ stated in *Corfu Channel*:

> '[I]t cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known'[409]

In cyberspace, the UN GGE Report 2015 similarly asserted:

> '[T]he indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State.'[410]

While the reference concerns attribution it also suggests that it is insufficient to attribute knowledge based on the mere fact that a cyber operation emanated from a state's territory as attribution also requires knowledge of

407 See chapter 2.A.IV; see also Giulio Bartolini, 'The Historical Roots of the Due Diligence Standard', in Heike Krieger/Anne Peters/Leonhard Kreuzer (eds.), *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 23–41, at 38.

408 ICJ, Separate Opinion of Judge Alvarez (n. 312), p. 44, para. 4.

409 ICJ, *Corfu Channel Case (United Kingdom v. Albania)*, Judgment of 9 April 1949, ICJ Reports 1949, 4, p. 18.

410 UN GGE Report 2015, para. 28f.

the relevant facts.[411] Hence, in line with the ICJ judgment in *Corfu Channel,* the fact that a cyber operation emanated from the territory of a state does not create a rebuttable presumption that the state knew.[412]

2. Duty to have known under the harm prevention rule

It would however be inadequate if a state could merely point to its lack of actual knowledge regarding the harmful activity and hereby evade accountability. The ICJ asserted in *Corfu Channel*:

> '[T]hat a State on whose territory or in whose waters an act contrary to international law has occurred, may be called upon to give an explanation. […] [A] State cannot evade such a request by limiting itself to a reply that it is ignorant of the circumstances of the act and its authors'.[413]

Hence, states are held accountable for what they know, but also for what they should know. Judge *Alvarez* asserted this in his Separate Opinion in the case:

> '[E]very State is considered as having known, or as having a duty to have known, of prejudicial acts committed in parts of its territory where local authorities are installed; that is not a presumption, nor is it a hypothesis, it is the consequence of its sovereignty.'[414]

Alvarez hereby expresses the 'constructive knowledge' rationale based on which a state's knowledge is imputed, regardless of whether actual knowledge existed. This is justified as knowledge was obtainable through the exercise of available means, in this case through installed authorities.[415] In a similar vein, the ILC reiterated in its commentaries to the Draft Articles on Prevention that a state needs to take 'reasonable efforts to inform itself of

411 ILC, Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), UN General Assembly, A/56/10, 23 April-1 June, 2 July-10 August 2001, commentaries to art. 2, p. 35, para. 4.

412 Coco/Dias, 'Cyber Due Diligence' 2021 (n.63), 789; however arguing for such a rebuttable presumption Wolf Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace', in Christian Czosseck/Rain Ottis/Katharina Ziolkowski (eds.), *International Conference on Cyber Conflict* (2012) 7–19, at 17.

413 ICJ, *Corfu Channel* (n. 409), p. 18.

414 ICJ, Separate Opinion of Judge Alvarez (n. 312), p. 44, para. 3.

415 See chapter 2.A.IV.

factual and legal components that relate foreseeably to a contemplated procedure (…)'.[416] It also stated that due diligence requires taking appropriate measures to identify risky activities.[417]

Acquiring knowledge about the risk of harm can also be a due diligence requirement under the duty to protect in international human rights law. The ECtHR for example required the establishment of observation posts to enable the state to warn the public about impending, possibly life-threatening dangers.[418] The UN Human Rights Committee noted that 'supervision' may be required in order to prevent and punish perpetrators.[419] It is hence clear that due diligence for harm prevention, as well as due diligence under human rights law, may require states to proactively acquire knowledge about potentially risky behaviours.

States have broadly recognized that the constructive knowledge standard applies in cyberspace. The Netherlands for example acknowledged the applicability of the constructive knowledge standard.[420] Also a report of the CoE pointed at monitoring measures for discharging due diligence obligations – or in the words of the report 'reasonable efforts by a state to inform itself of factual and legal elements'.[421] Moreover, the UN GGE Report 2021 recognized that due diligence may require states to acquire information.[422] Only New Zealand explicitly advocated against the applicability of the constructive knowledge standard and argued that only in the case of actual

416 ILC Draft Articles on Prevention 2001 (n. 31), commentary to art. 3, p. 154, para. 10.
417 Ibid.
418 ECtHR, *Case of Budayeva and Others v. Russia*, Judgment of 20 March 2008, Application Nos 15339/02 et al., para. 156.
419 UN Human Rights Committee, 'General Comment 36' (n. 76), para. 21.
420 Netherlands, 'International Law in Cyberspace' 2019 (n. 32), p. 4.
421 Steering Committee on the Media and New Communication Services (CDMC), Explanatory Memorandum to the draft Recommendation CM/Rec(2011) of the Committee of Ministers to member states on the protection and promotion of Internet's universality, integrity and openness, CM(2011)115-add1 24 August 2011, para. 82. The reference was made in relation to the 'universality and integrity of the Internet' but it supports the argument that also in the cyber context due diligence may require best efforts to acquire information.
422 UN GGE Report 2021, para. 29: 'This norm reflects an expectation that if a State is aware of or is notified in good faith that an internationally wrongful act conducted using ICTs is emanating from or transiting through its territory it will take all appropriate and reasonably available and feasible steps to detect, investigate and address the situation'.

knowledge a state would be required to act with due diligence.[423] It provided no further reason for its position, but the context of the statement suggests that New Zealand was concerned about a potential push towards extensive monitoring of cyber activities.[424] Yet, the question if and to which degree a state needs to monitor cyber activities is a secondary question and requires careful balancing[425] that should not be precluded by negating the constructive knowledge standard from the outset. Hence, it can be assumed that constructive knowledge suffices in cyberspace and that, consequently, due diligence may require states to acquire knowledge.[426]

3. Content of a duty to have known in cyberspace

Constructive knowledge is defined as 'knowledge that one using reasonable care and diligence should have, and therefore is attributed by law to a given person [or State]'.[427] The UN GGE 2021 highlighted that states are not required to 'monitor all cyber activities'[428], hereby reflecting the scepticism of New Zealand regarding the constructive knowledge standard. It stated that:

> 'The norm raises the expectation that a State will take reasonable steps within its capacity to end the ongoing activity in its territory through means that are proportionate, appropriate and effective and in a manner consistent with international and domestic law. Nonetheless, it is not expected that States could or should monitor all ICT activities within their territory.'[429]

423 New Zealand, The Application of International Law to State Activity in Cyberspace, 1 December 2020, para. 17.
424 Ibid.
425 On the requirement to interpret due diligence in compliance with other international legal rules, including human rights law, see above chapter 4.B.III.
426 Karine Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations' *Baltic Yearbook of International Law* 14 (2014), 23, 28; Coco/Dias, 'Cyber Due Diligence' 2021 (n. 63), 793.
427 Bryan A. Garner, in Henry Campbell Black (founder), *Black's Law Dictionary* (St. Paul (MN): West Publishing 10th ed. 2014).
428 New Zealand, 'International Law in Cyberspace' 2020 (n. 423); para. 17; Bannelier/Christakis, 'Prevention Reactions' 2017 (n. 151), p. 20.
429 UN GGE Report 2021, para. 30a.

Similarly, Ecuador argued in its UN OEWG 2020 submission that

> 'this norm should not be interpreted as requiring a state to monitor proactively all ICTs within its territory'.[430]

With regard to authoritarian tendencies to exercise strict control over cyberspace and in particular strict content control, concerns of over-monitoring via an extensive interpretation of due diligence requirements seem well-founded. Yet, they should not be overemphasized.[431] As the ICJ stated in *Bosnia Genocide:*

> 'It is clear that every State may only act within the limits permitted by international law'[432]

Hence, a due diligence duty to acquire information about risks of harm would need to be interpreted in compliance with other rules of international law, in particular with human rights law. As a duty to monitor *all* ICT would violate international human rights law[433] due diligence does not require such monitoring.

Yet, ending the subject matter at this point, as is often done, does not seem satisfactory. It is worthwhile to analyse circumstantial evidence that courts have accepted in order to conclude on which level of knowledge a state ought to have in cyberspace.

In the *Corfu Channel* case based its assumption of constructive knowledge inter alia on the fact that Albania was monitoring its territorial waters closely.[434] In the *Bosnia Genocide* case the ICJ Judge *Keith* considered a number of criteria and specific circumstances, like overall role and specific relationships of various actors, in order to conclude that Miloševic on behalf of the Serbian state 'must have known'. These examples make clear that circumstantial evidence may suffice and that various international tribunals have shown leniency and 'liberal recourse to interferences of fact and circumstantial evidence'.[435]

---

430 Ecuador, 'Preliminary comments' 2020 (n. 192), p.2.
431 Buchan, 'Obligation to Prevent' 2016 (n. 88), 442.
432 ICJ, 'Bosnia Genocide' 2007 (n. 39), para. 430; see also above chapter 4.B.III.
433 Buchan, 'Obligation to Prevent' 2016 (n. 88), 442; Delerue, 'Cyber Operations' 2020 (n. 47), 362.
434 ICJ, *Corfu Channel* (n. 409), p. 18, 19: 'It is clearly established that the Albanian Government constantly kept a close watch over the waters of the North Corfu Channel'.
435 Monnheimer, 'Due Diligence ' 2021 (n. 36), 121; ICJ, *Corfu Channel* (n. 409), p. 18.

Applying such circumstantial evidence in the cyber context, one may argue that a significant increase in bandwidth[436] may indicate that a state ought to have known. Further criteria may be that a certain commonly known signature was used[437], unusual password activity[438], unusually huge data transfers, unusual traffic data[439], or an unusual range of IP addresses used.[440] Furthermore, the organizational proximity of a state to an actor, e.g. an intelligence unit, may be considered a relevant factor in attributing constructive knowledge, regardless of the question whether actions of such actors can be attributed or if a state is complicit in it. Other circumstantial evidence may be that a state routinely operates investigative measures that should regularly detect the malicious operation in question[441], that governmental infrastructure was used[442], or that it in a specific case conducted a law-enforcement measure.[443]

4. Practical implications

In practice, this requires that a state uses the channels of acquiring knowledge that it already has in place.[444] In doing so, it needs to comply with other rules of international law.[445] Divergences between states are likely as 'active anticipation and constant vigilance' can be cost-intensive.[446] Developing states may lack the technological capacity to acquire knowledge in

436 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 14), commentary to rule 6, p. 41, para. 40.
437 UK, Department for Business Innovation & Skills, Guidance, 10 Steps: Monitoring, 16 January 2015, available at: https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-monitoring--11.
438 US, National Institute of Standards and Technology (NIST), Manufacturers Guide to Cybersecurity, For Small and Medium-Sized Manufacturers, 2019, p. 21.
439 Delerue, 'Cyber Operations' 2020 (n. 47), 161.
440 UK, 10 Steps Monitoring (n. 437).
441 Buchan, 'Obligation to Prevent' 2016 (n. 88), 440.
442 Luke Chircop, 'A Due Diligence Standard of Attribution in Cyberspace', *International and Comparative Law Quarterly* 67 (2018), 1–26, at 8.
443 Lahmann Unilateral Remedies' 2020 (n. 146), 158.
444 Coco/Dias, 'Cyber Due Diligence' 2021 (n.63), 788; Delerue, 'Cyber Operations' 2020 (n. 47), 362; in so far concurring with ICJ, Separate Opinion of Judge Alvarez (n. 312), p. 44, para. 4.
445 Coco/Dias, 'Cyber Due Diligence' 2021 (n. 63), 789.
446 Stoyanova, 'Positive Obligations' 2020 (n. 71), 608.

cyberspace.[447] It is hence compulsory that states press ahead with capacity-building to keep technologically up to date.[448]

Furthermore, taking legislative measures is a measure that every state, regardless of capacity, can take.[449] States could set up channels for gaining knowledge, for example by stipulating domestic obligations to report or notify about cyber security incidents. Examples are the EU NIS 1 and NIS 2 directives which require member states to ensure that critical infrastructure operators report, without undue delay, incidents having a substantial impact on their services to the incident response teams or competent authorities.[450] Member states are also required to ensure that non-essential service providers are under an obligation to report incidents when they have a 'substantial impact'.[451] Reporting requirements of critical infrastructure operators are also recommended by international institutions.[452] Acquisition of knowledge could furthermore be achieved via legislation on retention and preservation of data in criminal proceedings. In this regard the due diligence requirement to acquire knowledge may converge with the due diligence requirement to put cyber investigative capabilities in place.[453] As state practice and opinio iuris so far is not sufficiently consistent these examples of acquiring knowledge, as well as the requirement to press ahead with technological capacity-building, is currently rather to be considered best practice. Yet, as the bottomline, due diligence requires that states at least set up a basic infrastructure, via legislative and administrative measures, that brings them into the position to acquire knowledge of harmful

447 Eric Talbot Jensen/Sean Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?', *Texas Law Review* 95 (2017), 1555–1577, at 1574.

448 Coco/Dias, 'Cyber Due Diligence' 2021 (n. 63), 794.

449 ILC Draft Articles on Prevention 2001 (n. 31), commentaries to art. 3, p. 155, para. 17: 'Vigilance, employment of infrastructure and monitoring of hazardous activities in the territory of the State, which is a natural attribute of any Government, are expected.'

450 EU, NIS 2 directive (n. 275), art. 23 (1); see also already before the repealed directive EU, Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS 1 directive), art. 14 (3).

451 NIS 2 directive (n. 275), art. 23 (1); before already NIS 1 directive (n. 450), art. 16 (3).

452 ITU, Guide to Developing a National Cybersecurity Strategy, 2018, p.25.

453 See above chapter 4.D.I.5.1.

cyber activities and to hereby 'keep being informed' about activities on their territory.[454]

III. Critical infrastructure protection

States are highly concerned about cyber harm to critical infrastructure.[455] As a measure of institutional capacity-building, due diligence may require states to protect their *own* critical infrastructure against risks of cyber harm.

1. Duty to protect own critical infrastructure against cyber harm

Para. 13 lit. g of the UN GGE Report 2015 stipulates that states should protect *their* critical infrastructure.[456] This norm was endorsed by the UN General Assembly[457], and similarly reasserted in the UN OEWG.[458] Despite this endorsement it is unclear whether the duty to protect is a due diligence requirement under the harm prevention rule, a due diligence requirement under human rights law, or an autonomous distinct duty to protect.[459]

1.1 Spill-over effects of cyber harm to critical infrastructure

Protecting own critical infrastructure against cyber harm is in the self-interest of states. However, cyber operations against critical infrastructure of one state can have ramifications internationally. The UN GGE Report 2021

454 Buchan, 'Obligation to Prevent' 2016 (n. 88), 441.

455 See above chapter 3.C.II; regarding the negative prohibitive dimension of the harm prevention rule requires states to abstain from impairing critical infrastructure of other states, see above chapter 4.A.I.

456 UN GGE Report 2015, para. 13g: 'States should take appropriate measures to protect their critical infrastructure from ICT threats (…).'

457 UN General Assembly Resolution A/RES/73/27, 5 December 2018, para. 1.7.

458 UN OEWG, Final Report, para 31: 'States should continue to strengthen measures to protect of all critical infrastructure from ICT threats, and increase exchanges on best practices with regard to critical infrastructure protection.'

459 Highlighting that protection of critical infrastructure from cyber threats is both in the interests of individuals on the territory as well as of other states due to spillover effects Gross, 'Cyber Responsibility' 2015 (n. 196), 493.

highlighted potential spill-over effects of cyber harm to critical infrastructure:

> '(…) ICT activity that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public can have cascading domestic, regional and global effects.'[460]

Also the UN GGE Report 2015 already recognized that impairment of critical infrastructure vulnerabilities may transcend national borders.[461] The potential transboundary dimension of impairment of critical infrastructure operation is also acknowledged in the EC Directive 2008/114 which introduces the category 'European Critical Infrastructure'.[462] Reflecting this international dimension of critical infrastructure protection, the Netherlands underlined that the adequate protection of critical infrastructure in one state benefits the international community[463], hereby e.g. concurring with *Gross*.[464]

It is hence clear that in many cases cyber harm to the critical infrastructure of one state may also affect the legally protected interests of other

460 UN GGE, Report 2021, para. 42.

461 UN GGE Report 2015, para. 16 d; also the ILA, 'Cybersecurity and Terrorism' 2016 (n. 65), para. 244; Tyson Macaulay, 'The Danger of Critical Infrastructure Interdependency', *Center for International Governance Innovation,* 2019, available at: https://www.cigionline.org/articles/danger-critical-infrastructure-interdependency/.

462 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Rc. 7: 'There are a certain number of critical infrastructures in the Community, the disruption or destruction of which would have significant cross-border impacts. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructures.'

463 Netherlands' response 2020 (n. 30), para. 28: '(…) to address the development that critical infrastructure is no longer confined to the borders of States alone the report should acknowledge that critical infrastructure is increasingly becoming transnational and interdependent and that adequate protection of these critical infrastructures would benefit the international community.'

464 Gross, 'Cyber Responsibility' 2015 (n. 196), 493: 'In a digitally interconnected world, the strength of the digital chain may be only as strong as its weakest link. Cybersecurity incidents that compromise the security or the functionality of a network component in one country may have critical spillover impacts on the security or functionality of other parts of the network, or other networks that are connected or otherwise related to it, and that may directly or indirectly affect other states or non-state actors.

states. Yet, the degree to which interests of other states and the international community are affected by cyber operations against critical infrastructure diverges. For example, in the financial sector the interdependency is likely high: Disruptions of the stock market of one country may affect the stock market and financial services in other states. Disabling the national transport infrastructure, e.g. the national railway, via ransomware may also have spill over effects on other countries. Also impairment of the energy and transport sector is likely to affect the interests of other states.[465] But it cannot be presumed that any impairment of critical infrastructure *per se* affects the rights of other states. If e.g. a cyber operation disrupts the telecommunications services in the region of one state or if local transportation in only one particular city is impaired, a sufficient cross-border would likely lack. It seems hence reasonable to limit a due diligence duty to protect own critical infrastructure to the list of internationally recognized key critical infrastructures.[466] States may individually choose to designate further institutions as critical infrastructure but in such cases the interests of other states are likely not implicated.

1.2 Duty to protect critical infrastructure under human rights law

The duty to protect *own* critical infrastructure may furthermore be required under human rights law. Attacks on critical infrastructure can have severe harmful impacts on individuals. Operations against medical facilities or nuclear reactors may for example interfere with the right to life and the right to health.[467] In September 2020 a woman died after her medical treatment was interrupted by a cyber operation.[468] The exposure of individuals to potentially deadly cyber operations, e.g. against smart vehicles, is likely to

465 Council Directive 2008/114 (n. 462) establishes a procedure for identifying and designating European Critical Infrastructures (ECIs) in the transport and energy sectors whose disruption would have significant cross-border impacts.

466 On key critical infrastructure see chapter 3.C.II.2.3.

467 Depicting impediment of medical treatment Germany following a ransomware attack against a hospital in Neuss, Germany, Bundesamt für Sicherheit in der Informationstechnik (BSI), *Schutz Kritischer Infrastrukturen* (2016), p. 6.

468 Mellisa Eddy/Nicole Pelroth,'Cyber Attack Suspected in German Woman's Death', *New York Times,* 18 September 2020, available at: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.

increase with the Internet of Things.[469] But cyber harm can also constitute a risk to economic and social rights. In July 2021, a ransomware operation crippled various agencies' capability to pay unemployment and parental aid in a region in Germany[470], leaving affected individuals without potentially vital financial support. Also the harmful consequences for individual of attacks against the financial system have been highlighted.[471] Hence, it is clear that cyber harm against critical infrastructure which constitute a risk to human rights also triggers due diligence duties to protect.[472]

1.3 Best practice standards for protecting critical infrastructure

Para. 13 lit. g of the UN GGE Report 2015 calls on states to exercise 'appropriate measures' to protect their critical infrastructure.[473] Which specific measures states are expected to take is not spelled out but a variety of best practice standards or recommendations exist. E.g. both the UN General Assembly Res. 58/199 of 2004 and the UN General Assembly Res. 64/211 of 2010 provide a 'voluntary self-assessment tool for national efforts to protect critical information infrastructure'.[474] Also the ITU has provided a ITU National Cybersecurity/Critical information infrastructure protection Self-Assessment Tool[475] and the OSCE has addressed critical infrastructure

469 Bannelier/Christakis, 'Prevention Reactions' 2017 (n. 151), 62.

470 Meike Laaff, 'Wie eine Cyberattacke einen ganzen Landkreis lahmlegt', *ZEITOnline*, 12 July 2021, available at: https://www.zeit.de/digital/datenschutz/2021-07/hackeran griff-anhalt-bitterfeld-cyber-katastrophenfall-kommunen-internetkriminalitaet.

471 US Department of Justice, 'Manhattan U.S. Attorney Announces Charges against Seven Iranians for Conducting Coordinated Campaign of Cyber Attacks against U.S. Financial Sector on Behalf of Islamic Revolutionary Guard Corps-Sponsored Entities', Press Release 24 Mach 2016: 'The charges announced today respond directly to a cyber-assault (…) The alleged onslaught of cyber-attacks on 46 of our largest financial institutions (…) resulted in hundreds of thousands of customers being unable to access their accounts (…)'.

472 ILA, 'Cybersecurity and Terrorism' 2016 (n. 65), para. 244.

473 UN GGE Report 2015, para. 13g; UN General Assembly Resolution A/RES/73/27, 11 December 2018, para. 1.7.

474 UN General Assembly Resolution A/RES/58/199, 23 December 2003, Annex Elements for protecting critical information infrastructures; UN General Assembly Resolution A/RES/64/211, Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, 21 December 2009, Annex, p. 3–5.

475 ITU National Cybersecurity/CIIP Self-Assessment Tool, Draft April 2009.

protection measures as CBMs.[476] On the national level, various policies for critical infrastructure protection exist, e.g. in the US the 'Framework for Improving Critical Infrastructure Cybersecurity'.[477] Several of the suggested measures in these guidelines and implemented measures in state practice are worth pointing out.

1.3.1 Ensuring IT security standards

Laws in several countries, e.g. in the EU[478] or China[479], require that critical infrastructure operators meet IT security standards and employ the 'state of the art'.[480] The ITU recommends that states ensure that critical infrastructure operators meet internationally recognized minimum cybersecurity standards[481], a suggestion also reiterated by Canada which referred to 'minimum baseline requirements'.[482] States are well advised to focus on what they consider the minimum requirement of critical infrastructure, e.g. via reference to technical standards, such as ISO, with due consideration of capacity limits of developing countries. One method of raising cyber

476 OSCE, Permanent Council Decision No. 1202, PC.DEC/1202, 10 March 2016, paras. 12–16; OSCE, Permanent Council Decision PC.DEC/1106, 3 December 2013, paras. 1–11.

477 NIST, 'Framework for Improving Critical Infrastructure Cybersecurity 1.1', available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

478 EU, NIS 2 Directive (n. 275), art. 21 (1): 'Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures (…) Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures (…) shall ensure a level of security of network and information systems appropriate to the risks posed (…).

479 Cybersecurity Law of the People's Republic of China, 1 June 2017, art. 23: 'Critical network equipment and specialized cybersecurity products shall follow national standards and mandatory requirements, and be security certified by a qualified establishment or meet the requirements of a security inspection, before being sold or provided (…).'

480 Highlighting the importance of harmonizing technical standards of critical infrastructure Michael Berk, 'Recommendation 13g and h', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 191–222, at 205.

481 ITU, 'Guide National Cybersecurity Strategy' 2018 (n. 452), p. 43.

482 UN OEWG Chairs Summary 2021 (n. 273), Annex, Canada, p. 13.

security standards may be certification.[483] An important area of adhering to security standards is emergency preparedness.[484]

1.3.2 Criminal legislation

The UN General Assembly[485], the AU Malabo Procotol[486], as well as commentators have underlined that enacting cybercrime legislation is an important tool for protecting one's critical infrastructure.[487] A UN Study in 2013 found that the character of an ICT system attacked as critical infrastructure is an aggravating circumstance in a large number of countries[488], leading to higher penalties. As critical infrastructure is regularly threatened by cyber operations that constitute data or system interference – which states are required to criminalize due to due diligence[489] – due diligence for critical infrastructure protection converges with the due diligence requirement to criminalize.

1.3.3 Inter-state and public-private cooperation

The UN OEWG Final Report broadly referred to the need for cooperation in the context of protection of critical infrastructure[490], similar to France which called for cooperation against risks to critical infrastructure[491] and China which called for exchanges on emergency coordination regarding threats to critical infrastructure.[492] Also the UN Security Council highligh-

483 China, 'Cybersecurity Law' 2017 (n. 481), art. 23; highlighting that certification of critical infrastructure is critical EU, 'Cybersecurity Act' 2019 (n. 261), rc. 65.
484 ILA, 'Cybersecurity and Terrorism' 2016 (n. 65), para. 247.
485 UN General Assembly Resolution A/RES/64/211, 21 December 2009, para. 13–16.
486 Malabo Convention (n. 328), art 25 (4).
487 David P. Fidler, 'Whither the Web?: International Law, Cybersecurity, and Critical Infrastructure Protection', *Articles by Maurer Faculty* 2452 (2015), at 2456; ILA, 'Cybersecurity and Terrorism' 2016 (n. 65), para. 269.
488 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 85.
489 See above chapter 4.D.I.4.2.
490 UN OEWG Final Report 2021, para. 59: 'Capacity-building aimed at enabling States to identify and protect national critical infrastructure and to cooperatively safeguard critical information infrastructure was deemed to be of particular importance.'
491 France, Stratégie internationale de la France pour le numérique, 2017, p. 32.
492 China, Cyber Attacks Against Critical Infrastructure' (n. 8); see also Foreign Ministry Spokesperson Geng Shuang's Regular Press Conference on April 24, 2020:

ted the need for inter-state cooperation against cyber operations.[493] The substance of such cooperation for critical infrastructure in cyberspace remains undefined but it is to be assumed that at least the procedural due diligence requirements – all of which are underpinned by the normative aspiration of cooperation[494] – also apply with regard to critical infrastructure.

Lastly, as private actors operate the large majority of critical infrastructure, cooperation between private and public actors, e.g. through notification obligations on private actors, as well as regulation of the private sector[495], is crucial for effectively protecting a state's own critical infrastructure.

1.4 Non-binding best practice standards

Commentators have labelled these measures the soft law of critical infrastructure protection.[496] They are hence not binding due diligence requirements but rather best practices for discharging the due diligence obligation to protect *own* critical infrastructure. In particular, establishing minimum security standards for critical infrastructure seems crucial for reducing cyber insecurity. While limited technological capacity will pose a challenge for some states the argument that an objective minimum standard of IT security with regard to critical infrastructure is emerging is particularly strong.

'States should increase exchanges on standards and best practices with regard to critical infrastructure protection, and explore the possibilities to establish relevant risk early warning and information sharing mechanism [and] to improve protection capability for cyber security of states (…).'

493 UN Security Council, S/RES/2341, 13 February 2017, para. 1: Encourages all States to make concerted and coordinated efforts, including through international cooperation, to raise awareness, to expand knowledge and understanding of the challenges posed by terrorist attacks, in order to improve preparedness for such attacks against critical infrastructure.

494 See chapter above 4.C.I.

495 UN GGE Report 2021, para. 49; India, Latest Edits to Zero Draft, 2021, para. 21.

496 Fidler, 'Wither the Web' 2015 (n. 487), 2465; on the soft law character of state practice regarding protection of critical infrastructure ILA, 'Cybersecurity and Terrorism' 2016 (n. 65), para. 243.

2. Duty to prevent cyber harm to the critical infrastructure of other states

For the sake of comprehensiveness, it is to be noted that due diligence requires not only to protect own critical infrastructure but also to take reasonable and appropriate measures to prevent cyber harm to the critical infrastructure of other states. This clarification is due to the fact that even states which have asserted a negative obligation not to damage other state's critical infrastructure, such as China, have notably fallen short of asserting a duty to prevent malicious acts against the critical infrastructure of other states.[497] Only Iran has expressly acknowledged a duty to prevent harm to the critical infrastructure of other states.[498] Overall, states avoid explicit commitments to prevent cyber harm to the critical infrastructure of other states. Yet, there is no teleological reason why preventive due diligence requirements and in particular procedural due diligence obligations should not apply to cyber operations against critical infrastructure of other states. Cyber harm to critical infrastructure is consistently highlighted by states as particularly harmful.[499] Also para. 13 lit. h of the UN GGE Report 2015 requires states to 'respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts'[500], indicating that states recognize their responsibility to mitigate cyber risk to the critical infrastructure of other states. Also the assertion by China which highlighted the importance of early warning regarding cyber risks to critical infrastructure[501] further underscores the acknowledgment of the necessity to mitigate transboundary risks to critical infrastructure. States are well advised to distinguish and commit more clearly between preventive obligations and best practices for the protection of their *own* critical infrastructure and the duties to prevent harm to the critical infrastructure of other states.

497 UN OEWG Chairs Summary 2021 (n. 273), Annex, China, p. 15.

498 Iran, Zero draft report of the Open-ended working group On developments in the field of information and telecommunications in the context of international security, UN OEWG, January 2021, p. 13: 'All forms of interventions and interference or attempted threat against (…) cyber related critical infrastructure of the states shall be condemned and prevented'.

499 See chapter 3.C.III.

500 UN GGE Report 2015, para. 13h.

501 China, Foreign Ministry, 'Press Conference' 2020 (n. 492): 'States should (…) explore the possibilities to establish relevant risk early warning and information sharing mechanism (…) in case of cyber attacks against critical infrastructure.'

IV. The establishment of computer emergency response teams and points of contact for international cooperation

In the international legal discourse both CERTs, as well as national points of contact are frequently mentioned in discussions on the UN level, e.g. in the UN GGE[502] or UN OEWG reports[503], or in individual statements of states.[504] Also commentators have acknowledged the importance of CERTs.[505] This raises the question whether due diligence for harm prevention requires the establishment of both CERTs, as well as generally the establishment of national points of contact.

1. Divergent understandings of emergency response teams and points of contact

CERTs are institutions for incident response and mitigation in emergencies.[506] The UN GGE Report 2021 circumscribed CERTs as

> 'essential to effectively detecting and mitigating the immediate and long-term negative effects of ICT incidents'[507]

The definition of 'points of contact' partially overlaps with the CERT. First, CERTs are international point of contact during cyber incidents, as

502 UN GGE Report 2021, para. 21; UN GGE Report 2015, para. 13k.
503 UN OEWG, Pre-Draft Report 2020, para. 44.
504 Cuba, Considerations on the Initial Pre-Draft of the Open-Ended Working Group, 2020, p. 3; Canada's implementation of the 2015 GGE norms 2019 (n. 166), p. 13.
505 Woltag, 'Cyber Warfare' 2014 (n. 212), 69.
506 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 14), Glossary, p. 563: 'A team that provides initial emergency response aid and triage services to the victims or potential victims of 'cyber operations' (see below) or cyber crimes, usually in a manner that involves coordination between private sector and government entities'; Roy Schondorf, Israel Ministry of Justice, Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations, 8 December 2020: 'CERTs are already doing what could arguably fall into th[e category of due diligence][addition by the author]: exchanging information with one another, as well as cooperating with each other in mitigating incidents'. CERTs as 'authorized emergency response teams', see UN GGE Report 2015, para. 13k.
507 UN GGE Report 2021, para. 65.

highlighted by states[508] or in cybercrime treaties.[509] Second, further 'points of contact' beyond CERTs exist, such as contact points for 'diplomatic, policy, legal and technical exchanges'[510], or for information exchange and assistance in investigations.[511] The notion of points of contact is hence amorphous and not to be understood as a technical legal term but rather – in the very meaning of the word – as context-dependent points of contact. It is hence necessary to take the context and a certain degree of ambiguity into account when assessing references to CERTs and points of contact in international legal practice.

2. Establishment of CERTs and points of contact as a due diligence requirement

Establishing a national CERT as a capacity-building measure could be considered a due diligence measure envisioned by Art. 16 of the ILC Draft Prevention Articles which requires emergency preparedness (i.e. contingency plans to respond to incidents).[512] It could also be grasped under Art. 5 of the Draft Prevention Articles which requires the establishment of the necessary legislative, administrative or other action.[513]

States and commentators have highlighted the importance of establishing a CERT or a national point of contact for cyber risk mitigation and have also linked it to due diligence. South Korea for example suggested that designation of a national point of contact by the UN OEWG would be worthwhile to discharge due diligence.[514] Israel similarly referred to CERTs

508 Australia, 'Cyber Engagement Strategy' 2017 (n. 149), p. 25; New Zealand, Cyber security strategy 2016, Action Plan Annual Report, p. 2: 'CERT NZ will be the international point of contact for cyber security matters, working closely with CERTs in other countries to prevent and respond to cyber security incidents'.

509 Convention on Cybercrime 2001 (n. 215), art. 35.

510 UN OEWG Final Report, para. 47.

511 UN GGE Report, para. 17b.

512 ILC Draft Articles on Prevention 2001 (n. 31), art. 16: 'The State of origin shall develop contingency plans for responding to emergencies, in cooperation, where appropriate, with the State likely to be affected and competent international organizations.'

513 Ibid., art. 5: 'States concerned shall take the necessary legislative, administrative or other action including the establishment of suitable monitoring mechanisms to implement the provisions of the present articles.'

514 Republic of Korea, 'Comments' 2020 (n. 30), p. 5.

in the context of due diligence.[515] Also Guatemala has asserted that states are required to establish a CERT.[516] Ecuador has asserted that establishment of CERTs is crucial for identifying harmful activities and directly linked such establishment to due diligence in cyberspace.[517] The UN OEWG Final Report reiterates that a national point of contact is 'invaluable' and helpful for other CBMs.[518]

The UK referred to its designation of a national point of contact with regard to its implementation of the para. 13 UN GGE 2015 norms.[519] Already in 2008, the Arab states discussed that countries should establish a CERT for incident response.[520] Regarding alleged ransomware operations emanating from Russian soil US president Biden underlined the setting up of communication channel as instrumental for effective ransomware prevention

> 'United States expects when a ransomware operation is coming from [Russia's] soil – even though it's not sponsored by the state – we expect [Russia] to act (…) We've set up a means of communications now, on a regular basis, to be able to communicate to one another when each of us thinks something's happening in the other country.'[521]

Commentators have also pointed out that a point of contact is necessary for exchanges about vulnerabilities and remedies.[522]

There is hence overall strong evidence of increasing state practice and opinio iuris which affirms the importance of CERTs for risk mitigation and prevention in cyberspace, inter alia through procedural due diligence

515 Schondorf, 'Israel's Perspective' 2020 (n. 506).
516 Organization of American States, Improving Transparency — International Law and State Cyber Operations: Fourth Report (Presented by Prof. Duncan B. Hollis), CJI/doc. 603/20 rev.1 corr.1, 5 March 2020, p. 20, para. 58.
517 Ecuador, 'Preliminary comments' 2020 (n. 192), p. 2.
518 UN OEWG Final Report, para. 47.
519 UK, 'Efforts to Implement Norms' 2019 (n. 87), p. 15.
520 ITU, 'Arab States call for heightened cybersecurity', Press Release on Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection on 18–21 February 2008 in Doha: 'Participants called for each country to create a national focal point for monitoring and responding to breaches in cybersecurity. Typically, this would take the form of a national computer security incident response team (CSIRT)'.
521 Maegan Vazquez, 'Biden warns Putin during call that 'we expect him to act' on Russian ransomware attacks', *CNN*, 9 July 2021, available at: https://edition.cnn.com/2021/07/09/politics/biden-putin-call-syria-ransomware/index.html.
522 Tsagourias, 'Recommendation 13j' 2017 (n. 200), para. 38.

obligations. Non-state actors such as Microsoft, as well as the UN GGE Reports, have asserted that CERTs may even be designated national critical infrastructure.[523]

3. Establishment of CERTs and points of contact under binding and non-binding norms

The establishment of CERTs is also required under binding regional treaty law. Art. 35 of the Budapest Convention requires states to establish national points of contacts for immediate assistance and evidence collection.[524] The establishment of a national CERT is also required under art. 10 (1) of the NIS 2 Directive of the EU.[525] In state practice, networks of points of contact for cybercrime prosecution exist.[526] Such national points of contact are available on a 24/7 basis and provide immediate assistance in case of emergencies. Points of contacts for cybercrime cooperation hence resemble the function of CERTs mentioned at the UN level as responsible point of contact in emergencies.[527] The Draft Report of the Expert Group Cybercrime of 2020 notably urged states to 'strengthen networks of collaboration among CERTs', hereby suggesting the equivalence of CERTs and points of contact for cybercrime cooperation. States may hence consider to designate one institution as both a CERT envisioned in the UN GGE and point of contact stipulated by cybercrime treaties.

Despite the often indeterminate references in international legal practice this state practice highlights that the establishment of CERTs or national point of contact regarding cyber incidents is already largely presupposed by states. States are so far cautious to commit to establishing CERTs as legally

523 Microsoft, Protecting People in Cyberspace: The Vital Role of the United Nations in 2020, 4 December 2019, p. 4.

524 Convention on Cybercrime 2001 (n. 215), art. 35: 'Each Party shall designate a point of contact available on a twenty-four hour, seven-daya-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence (…)'.

525 EU, NIS 2 Directive (n. 275), art. 10 (1).

526 Highlighting their relevance for international cooperation Report Expert Group 2019 (n. 253), para. 10h.

527 Stipulating the point of contact under Art. 35 of the Budapest Convention as potential contact in case of emergencies Cybercrime Convention Committee (T-CY), Draft AP II, 2018 (n. 145), para. 8, p. 5.

binding obligation. References to CERTs are frequently made in legally ambiguous terms, e.g. as CBMs, in the UN GGE[528] or individual statements by states.[529] Also the Final Report of the UN OEWG explicitly asserted that establishment of a national points of contact as a CBM.[530] Yet, the persistent assumption of the existence of such CERTs as points of contacts[531], as well as their instrumentality for discharging other potential diligence obligations[532], such as e.g. to assist with regard to ongoing incidents, or to warn or to cooperate in cybercrime investigations strongly suggests to consider the establishment of CERT a binding due diligence requirement.[533] The reluctance of states may inter alia be due to uncertainty about the functions and responsibilities of such institutions. A global repository, as envisaged by the Netherlands[534], the Philippines[535] may further clarity in this regard.[536]

For the sake of comprehensiveness, it is to be noted that states are obliged not to cause harm or to prevent harm to the CERTs of *other* states. The negative prohibition is explicitly asserted in para. 13 lit. k of the UN GGE Report.[537]

528 UN GGE Report 2013, para. 26 lit. d; UN GGE Report 2015, para. 17c; UN GGE Report 2021, para. 76.
529 Netherlands' response 2020 (n. 30), paras. 33–36.
530 UN OEWG Final Report 2021, para. 47.
531 See e.g. African Union, Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, 29 January 2024 (endorsed by the Assembly of the AU on 18 February 2024), paras. 25, 66.
532 UN GGE Report 2021, para 27: 'Cooperation at the regional and international levels, including between national Computer Emergency Response Teams (CERTs)/ Computer Security Incident Response Teams (CSIRTs), the ICT authorities of States and the diplomatic community, can strengthen the ability of States to detect and investigate malicious ICT incidents and to substantiate their concerns and findings before reaching a conclusion on an incident.' UN OEWG, Final Report 2021, para. 47: 'As a specific measure, States concluded that establishing national Points of Contact (PoCs) is a CBM in itself, but is also a helpful measure for the implementation of many other CBMs, and is invaluable in times of crisis. States may find it useful to have PoCs for, inter alia, diplomatic, policy, legal and technical exchanges, as well as incident reporting and response'.
533 Woltag, 'Cyber Warfare' 2014 (n. 212), 106.
534 Netherlands' response 2020 (n. 30), para. 35.
535 Philippine Intervention on the Zero Draft, p. 1.
536 UN OEWG Chairs Summary 2021 (n. 273), para. 31.
537 See above chapter 4.A.II.

V. Evolving due diligence standard regarding institutional capacity

The preceding analysis has shown that due diligence requires a number of institutional safeguard measures as the organisational minimum standard. States cannot claim that they acted diligent if they have not enacted cybercrime legislation on key cybercrime offences or if they have not to established central cyber investigative measures. States are furthermore obliged to use existing channels of acquiring knowledge and also to establish certain basic channels of knowledge, e.g. via establishing reporting obligations on non-state actors. Furthermore, due diligence requires that states protect their *own* critical infrastructure, both under the harm prevention rule, as well as international human rights law. Due diligence for harm prevention also requires states to establish CERTs as points of contact in case of international cyber incidents, as well as points of contact for cybercrime cooperation. To relegate such measures to the level of non-binding guidelines[538] would not do justice to the indispensable function of such measures for fostering cyber resilience.

It is however to be cautioned that the required due diligence standard is not uniform and that states have discretion in implementing the precise requirements. Hence, with regard to all of the above-mentioned measures due diligence allows for divergences. With regard to the criminalization of states may e.g. choose to introduce *de minimis* requirements, criminalization exemptions for legitimate acts or additional criminalization requirements. With regard to cyber investigative measures states' divergences in technological capacity may soften the required standard. In establishing investigative capabilities states are required to install human rights safeguards. Regarding the required level of monitoring of cyber activities in a state's territory states are required to use the existing means of acquiring knowledge and, as a bottomline, to keep being informed about cyber activities in their territory. Ensuring appropriate IT security standards in critical infrastructure may be an emerging minimum standard of protecting one's own critical infrastructure but beyond this other protective measures can only be considered the 'soft law' of critical infrastructure protection. With regard to the establishment of CERTs and international points of contact

538 On criminalization of malicious cyber activities as a mere 'guideline' but not a binding requirement see Coco/Dias, 'Cyber Due Diligence Report' 2021 (n. 129), 202, 206.

the precise mode of establishment, function and responsibilities remains within a state's discretion.

Beyond these institutional capacity-building measures it is clear that in order to effectively discharge address risks of cyber harm states need to comprehensively and holistically address cyber security risks, e.g. via reassessing legislation including regulatory and liability regimes for network operators, telecommunication companies, or encryption services, or data security. To this aim, states have regularly adopted comprehensive cyber security strategies.[539] It is clear that at a minimum such strategies should systematically assess cyber risks. As an international standard for cybersecurity strategies can however not meaningfully be approximated, it cannot be considered a due diligence requirement.

539 See in more detail states' national strategies Coco/Dias, 'Cyber Due Diligence Report' 2021 (n. 129), 216, 217.

Chapter 5: Enforcement of the Harm Prevention Rule

A. Legal consequences of negligence

What if a state fails to comply with its procedural due diligence obligations or its diligence obligations regarding institutional capacity-building and hereby violates the harm prevention rule: Which rules apply? Under which circumstances can due diligence for harm prevention be enforced, for example via countermeasures?

Turning to the consequences of a violation of due diligence is worthwhile for two reasons. On the one hand, it is important for determining the potential and limits of due diligence and its compliance pull. On the other hand, a strict separation between reaction and prevention is elusive. Also reactive approaches have a future-oriented dimension, as can be seen in the *Trail Smelter* Arbitration.[1] In the words of *Duvic-Paioli*: The 'curative aspect reinforces the preventive rationale'.[2]

From the outset it has to be noted that, so far, state reactions to malicious cyber activities have mostly taken the form of diplomatic protests, political attribution, denial to save face[3], deterrent rhetoric and covert operations.[4] States have hardly ever pressed for norm compliance in the language of

1 Concluding on a violation of international law the tribunal ordered the instalment control measures to prevent future harm *Trail Smelter Case (USA v. Canada)*, Decision of 16 April 1938, UNRIAA, vol. III, 1966: '(…) in order to avoid damage occurring, the Tribunal now decides that a régime or measure of control shall be applied to the operations of the Smelter and shall remain in full force (…)'; see also chapter 2.A.V.2.

2 Leslie-Anne Duvic-Paoli, *The Prevention Principle in International Environmental Law* (Cambridge: Cambridge University Press 2018), 330.

3 Luke Chircop, 'A Due Diligence Standard of Attribution in Cyberspace', *International and Comparative Law Quarterly* 67 (2018), 1–26, at 24, 25.

4 Roguski has distinguished the 'responsive-deterrent' prong from the 'normative prong', Przemysław Roguski, 'An Inspection Regime for Cyber Weapons: A Challenge Too Far?, *AJIL Unbound* 115 (2021) 110–115, at 114, 115; Dan Efrony/Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice', *The American Journal of International Law* 112 (2018), 583–657, at 654: '[A]t this point in time, states seem to prefer to engage in cyberoperations and counteroperations "below the radar," and to retain, for the time being, some degree of stability in cyberspace by developing "parallel tracks" of restricted attacks, covert retaliation, and overt retorsion, subject to certain notions of proportionality.'

international law[5] or have turned to enforcement measures. No dispute over malicious cyber activities has been submitted to an international court. Even when states take the step to attribute harmful cyber operations, this attribution is not followed by a call for reparation or restitution.[6] For example, despite the attribution of the *WannaCry* attack to North Korea in December 2017 by the US and others, no claim for reparation or compensation was made.[7] When Australia attributed the *NotPetya* attack to Russia in February 2018, it merely referred to the need for deterrence.[8] Futhermore, when Australia publicly shamed an unnamed state actor for malicious cyber activities in 2020, it neither called for compensation nor announced countermeasures. It merely underlined the importance of cyber resilience.[9]

The decisions of the EU on restrictive measures against malicious cyber operations, based on the EU Cyber Restrictive Framework, are exceptional examples in which states have based their reaction to a cyber incident on legal criteria.[10] However, even these examples cannot strictly be seen as law

5 On the reluctance of states to clarify which international legal rule was violated see also François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press 2020), 415.

6 Noting the absence of claims for reparation and of taking countermeasures Chircop, 'A Due Diligence Standard' 2018 (n. 3), 11.

7 UK Foreign & Commonwealth Office, 'Foreign Office Minister condemns North Korean actor for WannaCry attacks', 19 December 2017, available at: https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks; 'U.S. blames North Korea for 'WannaCry' cyber attack', *Reuters,* 19 December 2017, available at: https://www.reuters.com/article/us-usa-cyber-northkorea-idUSKBN1ED00Q.

8 Australia, 'Australian Government attribution of the 'NotPetya' cyber incident to Russia', 16 February 2018: 'The Australian Government is (…) strengthening its international partnerships through an International Cyber Engagement Strategy to deter and respond to the malevolent use of cyberspace.'

9 Australia, Statement on malicious cyber activity against Australian networks, 19 June 2020: 'The Government encourages organisations, particularly those in the health, critical infrastructure and essential services, to take expert advice, and implement technical defences to thwart this malicious cyber activity.'

10 Council of the European Union, Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, Official Journal of the European Union, L 351 I; Council of the European Union, Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, L 246/12, Annex: '"Operation Cloud Hopper" targeted information systems of multinational companies in six continents, including companies located in the Union, and gained un-

enforcement measures, as they legally qualify as retorsion and hence do not presuppose that an internationally wrongful act has occured.[11] Therefore, it remains to be seen whether the law state responsibility and more generally the enforcement prong will be relevant in practice.

I. Harm not a constituent element of an internationally wrongful act

An important preliminary question is at which moment negligence under the harm prevention rule amounts to an internationally wrongful act based on which an affected state may press for norm compliance, take countermeasures, or institute judicial proceedings. To begin with, it is clear that in a case where harm occurs despite a state's best efforts to prevent it, the obligation is not violated.[12] Conversely, if harm occurs and a state is negligent the rule is violated. It is however not clear if an internationally wrongful act exists when a state acts negligent but no harm occurs. In other words, does mere negligence suffice for an internationally wrongful act?

The more dominant position is that harm is required. In the *Bosnia Genocide* case the ICJ held that the duty to prevent is only violated when harm actually occurs.[13] In the *Certain Activities* case it arrived at a similar result, albeit with a slightly divergent doctrinal reasoning. It distinguished the procedural obligation to exercise due diligence – which may be violated by mere negligence even without the occurrence of harm – from the substantive duty not to cause or to prevent harm – which is only violated in the case of harm.[14] The Tallinn Manual and other scholars have reiterated this

---

authorised access to commercially sensitive data, resulting in significant economic loss (…)'.

11 Thomas Giegerich, 'Retorsion', in Rüdiger Wolfrum (ed.), Max Planck Encyclopedia of Public International Law (Oxford: Oxford University Press 2011), para. 2. Tellingly, the EU classifies its restrictive measures as diplomatic measures and underlines that taking such measures does not imply the attribution of responsibility to a state, Council of the European Union, Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 7299/19, 14 May 2019, Rc. 2, 9.

12 See chapter 2.A.V.1.

13 ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment of 26 February 2007, ICJ Reports 2007, p. 43, para. 431.

14 ICJ, *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua), Construction of a Road in Costa Rica along the River San Juan (Nicaragua v. Costa Rica)*, Judgment of 16 December 2015, ICJ Reports 2015, p. 665, para. 226.

approach and assume an internationally wrongful act only in the case of harm.[15] These positions seem to reflect Art. 14 (3) ARSIWA which stipulates that a violation of an obligation to prevent occurs 'when the event occurs (…)'.[16]

The disadvantage of such an approach is obvious. If mere negligence does not suffice states cannot pressure a negligent state to act diligently by claiming a violation of international law. Due diligence would only become justiciable in the occurrence of harm, in other words when it is already too late. Such a result does not only seem undesirable, but also unintended: The commentaries to the ILC Draft Articles on Prevention explicitly acknowledge that the prevention article shall enable

> '(…) a State likely to be affected by an activity involving the risk of causing significant transboundary harm to demand from the State of origin compliance with obligations of prevention (…)'[17]

If negligence on its own did not constitute an internationally wrongful act this right to demand compliance acknowledged by the ILC would be undermined. Several commentators have hence criticized the approach of the ICJ.[18] As has been noted by ICJ Judges *Simma*, *al-Kaswahneh*[19] and

15 Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press 2017), commentary to rule 6, p. 46, para. 13; Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', *Journal of Conflict & Security Law* 21 (2016), 429–453, 450; Antonio Coco/Talita de Souza Dias, ''Cyber Due Diligence': A Patchwork of Protective Obligations in International Law', *European Journal of International Law* 32 (2021), 771–805, at 784.

16 ILC, Draft Articles on Responsibility of States for Internationally Wrongful Acts, UN General Assembly, A/56/10, 23 April-1 June, 2 July-10 August 2001, article 14 (3): 'The breach of an international obligation requiring a State to prevent a given event occurs when the event occurs and extends over the entire period during which the event continues and remains not in conformity with that obligation'.

17 ILC, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, UN General Assembly, A/56/10, 23 April-1 June, 2 July-10 August 2001, commentary to art. 1, p. 150, para. 6.

18 Jutta Brunnée, 'Procedure and Substance in International Environmental Law', *Recueil des Cours de l'Académie de Droit International de la Haye* 405 (2020) 77–240, 154, fn. 326; Andrea Gattini, 'Breach of the Obligation to Prevent and Reparation Thereof in the ICJ's Genocide Judgment", *European Journal of International Law* 18 (2007), 695–713, at 702.

19 ICJ, *Pulp Mills on the River Uruguay Case (Argentina v. Uruguay)*, Joint Dissenting Opinion of Judges al-Kaswahneh and Simma, ICJ Reports 2010, p. 108, 120, para. 26: 'Clearly in such situations, respect for procedural obligations assumes considerable

Greenwood[20] in the *Pulp Mills* case, as well as by ICJ Judge *O'Donoghue* in the *Certain Activities*[21] case, taking preventive measures is of particular importance for discharging the duty to prevent harm. Insisting on the occurrence of harm for a violation of the duty would not give appropriate weight to this crucial preventive dimension of due diligence[22] and may leave a 'glaring accountability gap'.[23] On the secondary level, the occurrence of harm may indeed be relevant – as pointed out by ICJ Judge *O Donoghue* harm is relevant for the question of the damages due[24] – but it is teleologically not convincing that a violation of the obligation to diligently prevent harm is not dependent upon it.[25]

This study therefore argues for taking a middle-ground: As argued elsewhere, an internationally wrongful act already occurs by mere negligence, provided that it is adequate in the circumstances.[26] Adequacy may be presumed in cases of complex situations which are difficult to ascertain or quantify, such as a state's duty to prevent corruption.[27] In such cases it

---

importance and comes to the forefront as being an essential indicator of whether, in a concrete case, substantive obligations were or were not breached. Thus, the conclusion whereby non-compliance with the pertinent procedural obligations has eventually had no effect on compliance with the substantive obligations is a proposition that cannot be easily accepted (…)'.

20 ICJ, *Pulp Mills on the River Uruguay Case (Argentina v. Uruguay)*, Separate Opinion of Judge Greenwood, ICJ Reports 2010, p. 221, 224, para. 9: 'It follows that a breach of these procedural obligations is a serious matter'.

21 ICJ, *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua), Construction of a Road in Costa Rica along the River San Juan (Nicaragua v. Costa Rica)*, Separate Opinion of Judge Donoghue, ICJ Reports 2015, p. 785, para. 9: 'In the planning phase, a failure to exercise due diligence to prevent significant transboundary environmental harm can engage the responsibility of the State of origin even in the absence of material damage to potentially affected States (…) I do not find it useful to draw distinctions between "procedural" and "substantive" obligations, as the Court has done.'

22 Brunnée, 'Procedure and Substance' 2020 (n. 18), 150: 'This conclusion neglects the true nature of the harm prevention rule. The rule is not primarily an obligation not to cause harm, but an obligation to take diligent steps to prevent harm'.

23 Anne Peters/Heike Krieger/Leonhard Kreuzer, 'Due diligence: the risky risk management tool in international law', *Cambridge Journal of International Law* 9 (2020), 121–136, at 130.

24 ICJ Certain Activities, 'Separate Opinion Donoghue' (n. 21), para. 9.

25 Alice Ollino, *Due Diligence Obligations in International Law* (Cambridge: Cambridge University Press 2022), 15, 208f.

26 Peters/Krieger/Kreuzer, 'Risky risk management' 2020 (n. 23), 129.

27 Ibid.; see already Anne Peters, 'Corruption as a Violation of International Human Rights', *European Journal of International Law* 29 (2018), 1251–1287, at 1261.

will be regularly challenging to assess the precise point at which a harmful consequence – the 'event' in the terminology of Art. 14 (3) ARSIWA – has occurred. Demanding the harmful consequence as a requirement for an internationally wrongful act would thereby effectively hollow out the possibility to enforce the law against malicious or harmful bevahiour. In such constellations it is appropriate to dispense with the requirement of harm and let mere negligence suffice for an internationally wrongful act.

In the cyber context, focussing on adequacy in the context of the harm prevention rule is suitable: It is for example complex and difficult to assess under which circumstances cyber harm is significant.[28] Insisting on harm occurrence here would substantially strip due diligence for harm prevention off its legal grip. Therefore, it can be assumed that mere negligence suffices for an internationally wrongful act.

II. Complementary applicability of the prevention rules and the rules on state responsibility

As the harm prevention rule does not lead to strict liability[29] it is noteworthy that the mere occurrence of harm despite due diligence compliance is not internationally wrongful and therefore does not implicate the law of state responsibility. The occurrence of harm however brings primary rules for harm mitigation into play, in particular the ILC Draft Principles on the Allocation of Loss which are stipulated to apply *after* the occurrence of harm, as opposed to the articles on prevention of harm which allegedly apply *before* the occurrence of harm.[30] These primary rules on risk mitiga-

28 See in more detail on various largely indeterminate categories of significant harm chapter 3.

29 See chapter 2.A.V.1.

30 The distinction in scope between the two ILC draft norm regimes is not clear-cut, both regimes partially overlap. Also the ILC draft principles on the allocation acknowledge that e.g. principle 5 on response measures is complementary to art. 16, 17 under the draft prevention articles. ILC, Draft Principles on the Allocation of Loss in the case of Transboundary Harm arising out of Hazardous activities, Report of the International Law Commission on the Work of its Fifty-Eighth Session, A/61/10, 1 May-9 June and 3 July-11 August 2006, commentary to principle 5, p. 84, para. 4; see also Heike Krieger/Anne Peters, 'Due Diligence and Structural Change in the International Legal Order', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 351–390, at 356.

tion and prevention are often termed the 'liability regime'.[31] Yet, this title is misleading as the predominant focus of both the ILC Draft Prevention Articles as well as the ILC Draft Principles on the Allocation of Loss lies on prevention and risk mitigation. To reflect this preventive and mitigatory dimension the term 'prevention regime' would therefore be more suitable.[32]

If a state acts negligent the law of state responsibility comes into play[33], regardless of whether harm has occurred.[34] Both the rules on state responsibility, as well as the primary rules on risk prevention and mitigation, apply then in a complementary manner. Such a complementary applicability is e.g. foreseen in Art. 29 ARSIWA[35] and also scholars have highlighted it.[36]

31 On reparatory and preventive requirements under the liability regime Attila Tanzi, 'Liability for Lawful Acts', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2010), para. 1; see also Rebecca Crootof, 'International Cybertorts: Expanding State Accountability in Cyberspace', *Cornell Law Review* 103 (2018), 565–644, at 599f.

32 Brunnée, 'Procedure and Substance' 2020 (n. 18), 156.

33 Henning Christian Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge: Cambridge University Press 2020), 153; Pierre-Marie Dupuy/Cristina Hoss, 'Trail Smelter and Terrorism: International Mechanism to Combat Transboundary Harm', in Rebecca M. Bratspies/Russell A. Miller (eds.), *Transboundary Harm in International Law: Lessons from the Trail Smelter Arbitration* (Cambridge: Cambridge University Press 2006), 225–239, at 227.

34 See above chapter 5.A.I.

35 ARSIWA, 2001 (n. 16), art. 29: 'The legal consequences of an internationally wrongful act under this Part do not affect the continued duty of the responsible State to perform the obligation breached'.

36 Allocation of Loss, 2006 (n. 30), commentary to principle 4, p. 77, para. 2; Brunnée, 'Procedure and Substance' 2020 (n. 18), 156, 157: 'The harm prevention regime and the State responsibility regime operate alongside one another They do so harmoniously, in the sense that the harm prevention regime specifies the primary obligations to which States are subject. The State responsibility regime comes into play when these primary obligations have been breached.'; see also Coco/Dias, 'Cyber Due Diligence' 2021 (n.15), 794: 'In this way, the no-harm principle is simultaneously a primary and secondary rule of international law: it requires states to take action and foresees the very consequences arising from a failure to act. Those consequences are, first, liability for the harm caused, and, secondly, responsibility for the eventual failure to redress it'; Jelena Bäumler, *Das Schädigungsverbot im Völkerrecht* (Berlin: Springer 2017), 16; Beatrice A. Walton, 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law', *Yale Law Journal* 126 (2017), 1460–1519, at 1487: '(…) like a secondary duty, it requires states to provide remedies when harms occur. This combination of duties comprises "liability" in international law. Liability is thus a "continuum of prevention and reparation" resulting from the underlying duty to prevent and redress transboundary harm.

Primary rules on risk prevention and mitigation resemble rules of state responsibility as also the former require states to provide remedies in the case of harm. Rules under both regimes can hence overlap. To give only one example of such a potential overlap of the two regimes: If a state has enacted insufficient cybercrime legislation, the establishment of cybercrime legislation is required under the law of state responsibility[37] and simultaneously by the continued duty to exercise due diligence for harm prevention.[38]

B. The content of state responsibility following negligence

As negligence constitutes an internationally wrongful act, the rules on the content of state responsibility in Art. 29ff. ARSIWA come into play. The ARSIWA are widely recognized as expressions of customary international law even though states have not yet turned them into a binding convention.[39] With regard to violations of the harm prevention rule in particular cessation, compensation as a way of reparation, and in some cases satisfaction may become relevant.

I. Compensation and reparation in cases of cyber harm

Art. 31 ARSIWA requires states to make reparation for the harm caused by the injury, i.e. a violation of due diligence.[40] The duty to provide for reparation was prominently asserted by the PCIJ in the *Chorzów* case and

37 ARSIWA, 2001 (n. 16), art. 30 lit. a: 'The State responsible for the internationally wrongful act is under an obligation: (a) to cease that act, if it is continuing'. The notion of an 'act' in the meaning of art. 30 ARSIWA also includes omissions, see ARSIWA, 2001 (n. 16), p. 31, fn. 33. The requirement to 'cease' the wrongful act under art. 30 lit. a ARSIWA hence simply means that a negligent state needs to enact the necessary cybercrime legislation and hereby 'cease' its wrongful omission.

38 See chapter 4.D.I.

39 ICJ, *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment of 26 February 2007, ICJ Reports 2007, p. 43, para. 420; Helmut Philipp Aust/Prisca Feihle, 'Due Diligence in the History of the Codification of the Law of State Responsibility', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 42–58, at 55.

40 ARSIWA, 2001 (n. 16), art. 31 (2): 'The responsible State is under an obligation to make full reparation for the injury caused by the internationally wrongful act (…) 2.

repeatedly reiterated by the ICJ.[41] As it is a customary rule it also applies in cyberspace, as highlighted e.g. by Switzerland.[42] Reparation requires to 'wipe out all the consequences of the illegal act and reestablish the situation which would, in all probability, have existed if that act had not been committed'.[43] It is recognized that both physical and non-physical harm can be the basis for compensation.[44] As cyber harm is often non-tangible[45] this is highly relevant in cyberspace.

It is difficult to assess the precise amount of harm which was caused by negligence. Often negligence occurs through omission. It is inherently difficult to determine if and to what extent an omission caused an injury, due to the so-called 'absence of facts'.[46] Usually, there is no direct causality between omission and the harmful effect.[47] Causality in cases of omissions

---

Injury includes any damage, whether material or moral, caused by the internationally wrongful act of a State'.

41 PCIJ, *Factory at Chorzów (Jurisdiction*), Judgment of 26 July 1927, Series A, No. 9, at 21; ICJ, *Case Concerning Armed Activities on the Territory of the Congo (DRC v. Uganda)*, Judgment of 19 December 2005, ICJ Reports 2005, p. 168, paras. 257, 259; ICJ, *Case concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia)*, Judgment of 25 September 1997, ICJ Reports 1997, p. 7, 81, para. 152; see also Delerue, 'Cyber Operations' 2020 (n. 5), 381ff.

42 Switzerland's position paper on the application of international law in cyberspace Annex UN GGE 2019/2021, May 2021, p. 7: 'If the aforementioned conditions exist and the state in question fails to fulfil due diligence requirements (…) The responsible state may also be required to make reparations.'; Australia, Australia's Cyber Engagement Strategy, Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace, 2019, p. 9.

43 PCIJ,' *Factory at Chorzów (Merits),* Judgment of 13 September 1928, Series A, No 17, at 47; see also Delerue, 'Cyber Operations' 2020 (n. 5), 381ff.

44 Schmitt, 'Tallinn Manual 2.0' 2017 (n.15), commentary to rule 28, p. 144, 145, para. 2; claiming compensation regarding non-material injury is however exceptional see e.g. ILC Survey of State practice relevant to international liability for injurious consequences arising out of acts not prohibited by international law, A/CN.4/384, ILC Yearbook 1985 vol. II(1)/Add., p. 108, para. 527.

45 See chapter I.C.I, II.

46 Rüdiger Wolfrum/Mirka Möldner, 'International Courts and Tribunals, Evidence', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2013), para. 64.

47 Sarah Heathcote, 'State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility', in Karine Bannelier/Theodore Christakis/Sarah Heathcote (eds.), *The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case* (London et al.: Routledge 2012), 295–314, at 310.

is therefore regularly normative causality.[48] With regard to due diligence omissions it regularly suffices that negligence increased the risk of harm[49] or that it has a proximal link.[50] Regarding the amount of damages due, the ILC has asserted that, as long as other harm is not severable from other causes or not remote, full compensation is due[51], concurring with the ICJ in *Corfu Channel* in which it held Albania responsible for its inaction and ordered it to pay full compensation although the precise chain of causality remained unclear.[52] Similarly, in *Tehran Hostages* Iran was held fully responsible for its failure to protect the US embassy, despite a combination of factors contributing to the incurred harm.[53] Some commentators have been more reluctant and argued that for cases of minor negligence a different assessment may be due.[54] An argument for such a more nuanced approach would be that compensation in the law of state responsibility does not entail a punitive element.[55] It also concurs with the observation that complementary responsibility of the affected state may reduce the amount of damages due.[56] In the *Gabčíkovo* case the ICJ stated:

48 Ibid.; 'Lahmann Unilateral Remedies' 2020 (n. 33), 188; Ollino, 'Due Diligence' 2022 (n. 25), 212.

49 Leonhard Kreuzer, 'Hobbesscher Naturzustand im Cyberspace? Enge Grenzen der Völkerrechtsdurchsetzung bei Cyberangriffen', in Ines-Jacqueline Werkner/Niklas Schörnig (eds.), *Cyberwar – die Digitalisierung der Kriegsführung* (Wiesbaden: Springer 2019), 63–86, at 82.

50 Walton, 'Duties Owed' 2017 (n. 36), 1465, fn. 25.

51 ARSIWA, 2001 (n. 16), commentary to art. 31, p. 93, para. 10; see also Lahmann, 'Unilateral Remedies' 2020 (n. 33), 191.

52 ICJ, *Corfu Channel Case (United Kingdom v. Albania)*, Judgment of 15 December 1949, ICJ Reports 1949, p. 10.

53 ICJ, *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgment of 24 May 1980, ICJ Reports 1980, 29–32; highlighting this aspect ARSIWA, 2001 (n. 16), commentary to art. 31, p. 93, para. 12.

54 Highlighting the particularly grave degree of negligence in the *Corfu Channel* and *Tehran Hostages* cases, hereby making full amount of compensation plausible Lahmann, 'Unilateral Remedies' 2020 (n. 33), 192.

55 ARSIWA, 2001 (n. 16), commentaries to art. 36, p. 99, para. 4.

56 ARSIWA, 2001 (n. 16), commentary to art. 31, p. 93, para. 11: 'A further element affecting the scope of reparation is the question of mitigation of damage. Even the wholly innocent victim of wrongful conduct is expected to act reasonably when confronted by the injury.'; see also ARSIWA, 2001 (n. 16), art 39: 'In the determination of reparation, account shall be taken of the contribution to the injury by wilful or negligent action or omission of the injured State or any person or entity in relation to whom reparation is sought.'

> 'It would follow from such a principle [of mitigation] that an injured State which has failed to take the necessary measures to limit the damage sustained would not be entitled to claim compensation for that damage which could have been avoided.'[57]

If, for example, a state protected its critical infrastructure only insufficiently against cyber harm, the compensation claim against a negligent state from which the cyber operation emanated would be accordingly reduced. Under which circumstances insufficient self-protection measures can be assumed needs to be assessed context-dependent. But if a state fails to discharge its due diligence obligations to protect human rights this regularly indicates that self-protection measures were insufficient. Beyond the duty to protect human rights – which is only the bottom line of what states are expected under the so-called 'duty to mitgate[58]' – it is e.g. plausible that failure to disclose a known vulnerability[59] would be considered insufficient self-protection. If the US had e.g. claimed compensation for the *WannaCry* attack from North Korea – and assuming that all other legal requirements for a reparation duty of North Korea were fulfilled – its claim arguably would have been reduced due to its belated disclosure of the Microsoft vulnerability.[60]

Beyond insufficient self-protection measures concurrent responsibility of other states may reduce the amount of damages due.[61] As cyber operations are often launched from various jurisdictions in some cases holding only one state accountable under the harm prevention rule would be inappropriate. Ascertaining whether and which compensation is due as a consequence of negligence will hence be regularly challenging.[62]

---

57 ICJ, *Gabčíkovo-Nagymaros* (n. 41), para. 80.

58 The duty to mitigate is not a primary obligation in the strict sense as failure to exercise does not entail state responsibility but may only 'preclude recovery to that extent', see ARSIWA, 2001 (n. 16), commentary to art. 31, p. 93, para. 11.

59 See in more detail on vulnerability disclosure as a potential due diligence requirement chapter 4.C.V.

60 See also with further examples Delerue, 'Cyber Operations' 2020 (n. 5), 396f.

61 On the relevance of contributory fault, ARSIWA, 2001 (n. 16), commentary to art. 31, p. 93, para. 12; ARSIWA, 2001 (n. 16), art 39: 'In the determination of reparation, account shall be taken of the contribution to the injury by wilful or negligent action or omission of the injured State or any person or entity in relation to whom reparation is sought'; see also regarding joint operations Schmitt, 'Tallinn Manual 2.0' 2017 (n.15), commentary to rule 28, p. 148, para. 12.

62 Highlighting the breadth of the notion of compensation Schmitt, 'Tallinn Manual 2.0' 2017 (n.15), commentary to rule 29, p. 150, para. 7.

II. Cessation

A negligent state is obliged to cease the violation – in the case of a due diligence violation its negligent behaviour – if it is continuing.[63] The obligation of cessation is therefore particularly relevant for obligations of a continuous character[64], such as the obligation to exercise due diligence under the harm prevention rule.[65] In the *Trail Smelter* case the tribunal e.g. required Canada to install 'a permanent régime (…) [to] effectively prevent future significant fumigations in the United States'[66]. In the cyber context, cessation may require a state to take measures of institutional capacity-building, e.g. to establish cybercrime legislation, cyber investigative measures or a national CERT.[67] Also with regard to procedural due diligence measures cessation may become relevant. The obligations to cooperate in cybercrime investigations, for instance, may, in cases of long-term investigations, have an extended temporal character. Cessation may in some cases also require assurance and guarantees of non-repetition.[68] Regularly, such assurances are not necessary as the principle of good faith leads to the presumption that a state will act legally in the future.[69] However, if a state has continuously denied a procedural obligation to take action against harmful cyber operations emanating from its territory, then arguably a state may seek assurances or guarantees from a state that it will comply with its procedural obligations in the future.[70] Scholars have highlighted that assurances may

63 ARSIWA, 2001 (n. 16), art. 30: 'The State responsible for the internationally wrongful act is under an obligation: (a) to cease that act, if it is continuing; (b) to offer appropriate assurances and guarantees of non-repetition, if circumstances so require.'

64 Delerue, 'Cyber Operations' 2020 (n. 5), 382.

65 Highlighting the relevance of cessation in cases of negligence Peters/Krieger/Kreuzer, 'Risky risk management' 2020 (n. 23), 130.

66 'Trail Smelter' (n. 1) 1934.

67 On due diligence obligations regarding institutional capacity see chapter 4.D.I–IV.

68 ARSIWA, 2001 (n. 16), art. 30b.

69 Delerue, 'Cyber Operations' 2020 (n. 5), 390.

70 See e.g. the statement of Russian president Putin acknowledging that hackers conduct activities from Russian territory while seemingly denying accountability of the Russian state in 2017: 'Hackers are free people, just like artists who wake up in the morning in a good mood and start painting. The hackers are the same. They would wake up, read about something going on in interstate relations and if they feel patriotic, they may try to contribute to the fight against those who speak badly', see Ian Phillips/Vladimir Isachenkov, 'Putin: Russia doesn't hack but "patriotic" individuals might', *APNews*, 1 June 2017. available at: https://apnews.com/article/moscow-donald-trump-ap-top-news-elections-international-news-281464d38ee54c6ca5bf573978e8

also take the form of a cyber policy change[71] or other diligence measures for institutional capacity-building.[72]

C. Countermeasures against negligence

When calls for cessation of negligence fail, injured states may resort to countermeasures.[73] Countermeasures are measures that would be unlawful if they were not taken in response to a prior violation of international law by the responsible state.[74] In the 'decentralized system' of international law countermeasures are a measure of self-help for injured states to restore the legal relationship with the responsible state.[75] In the cyber context, the UN GGE Report 2021 affirmed the applicability of the rules on countermeasures:

> 'An affected State's response to malicious ICT activity attributable to another State should be in accordance with its obligations under the Charter of the United Nations and other international law, including those relating to the settlement of disputes by peaceful means and internationally wrongful acts. (…)'[76]

ee91; such a position suggests that Russia will not mitigate future operations emanating from its territory. An affected state may in such circumstances demand assurances that Russia complies with its due diligence duty to stop or mitigate such operations when they occur. In the *Certain Activities* case the ICJ e.g. highlighted that Costa Rica had committed to diligent conduct (in this case to conduct an environmental impact assessment) in the future ICJ, 'Certain Activities' (n. 14), para. 173.

71 Delerue, 'Cyber Operations' 2020 (n. 5), 391.

72 Schmitt, 'Tallinn Manual 2.0' 2017 (n.15), commentary to rule 2, p. 143, para. 5.

73 ICJ, *Gabčíkovo-Nagymaros* (n. 41), para. 84; Walton, 'Duties Owed' 2017 (n. 36), 1515.

74 ARSIWA, 2001 (n. 16), p. 128, para. 1.

75 Ibid.

76 United Nations, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UN GGE), A/76/135, 14 July 2021 (UN GGE Report 2021), para. 25.

I. Purpose and proportionality requirements

Countermeasures need to comply with the 'purpose' requirement.[77] The purpose requirement limits countermeasures to induce norm compliance.[78] In the context of the harm prevention rule countermeasures are hence permitted for the sole purpose of inducing a targeted state to act diligently. Furthermore, countermeasures must be proportional and non-forcible.[79] They however do not need to be of the same kind. States may hence resort to countermeasures via non-cyber means following a violation of due diligence under the harm prevention rule.[80] Regarding proportionality the interconnectedness of cyberspace may lead to unforeseen effects of countermeasures on third parties.[81] States hence need to weigh well whether they aim to resort to countermeasures by cyber means.

Chircop has found these legal limitations regarding countermeasures following negligence unsatisfactory. Due to an alleged undue restriction of response possibilities by the purpose requirement he suggested that due diligence in cyberspace should be treated as a secondary rule of attribution.[82] The argument is mainly based on the perceived desirability of a larger arsenale for a response to a violation which would be restricted by the purpose requirement following the violation of due diligence as a primary rule.[83] If due diligence constituted a secondary rule of attribution, the negligent state would not only be held accountable for its negligence but for the harmful act itself – despite being neither supportive of nor complicit

77 Chircop, 'A Due Diligence Standard' 2018 (n. 3), 12.

78 ARSIWA, 2001 (n. 16), art. 49: 'An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations (…)'.

79 ARSIWA, 2001 (n. 16), art. 50 lit. 1a.

80 Michael N. Schmitt, 'In Defense of Due Diligence in Cyberspace', *Yale Law Journal Forum* 125 (2015), 68–81, at 79.

81 Schmitt, 'Tallinn Manual 2.0' 2017 (n.15), commentary to rule 2, p. 133, para. 1: '(…) in light of the interconnectedness of computer networks across borders, the effects of a countermeasure may reverberate throughout trans-border networks. When this occurs, the question is whether those effects violate obligations owed to third States or other parties.'

82 Chircop, 'A Due Diligence Standard' 2018 (n. 3), 11, 12: 'Were the due diligence principle to operate merely as a primary rule, the purpose and proportionality requirements would render ineffective the countermeasures available to harmed States'.

83 Ibid.

in it. As countermeasures can be taken in kind to the violating act[84] this would broaden the legal response options of an injured states.

However, the assumption that countermeasures would be unduly limited may be questioned. The legal limitations on countermeasures seem well justified in order to avoid an escalatory scenario which is particularly acute in cyberspace. Limiting countermeasures to negligence in addition still allows states to react in a proportionate manner to the negligence of another state. Moreover, if one assumed that due diligence constituted a secondary rule this would create a third category for the imputability of acts to states beside the rules on attribution[85] and complicity[86]. Such a consequence seems inappropriate. The blameworthiness of a negligent state is substantially different from a complicit state. A complicit state needs to have positive knowledge of the wrongful act while for a violation of due diligence mere constructive knowledge suffices.[87] Furthermore, complicity requires some form of positive action of a state while for negligence mere omission suffices.[88] For the same reasons, the blameworthiness of a negligent state seems even less comparable to a state which directs a harmful act or exercises effective control over it.[89] Due diligence should thus not be assessed as a secondary rule of attribution.[90] This concurs with the assertion of

84 ARSIWA, 2001 (n. 16), art. 49: 'An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations (…)'.

85 On rules for attribution see ARSIWA, 2001 (n. 16), art. 7–11.

86 Ibid, art. 16.

87 Ibid, art. 16 lit. a.

88 Maria Monnheimer, *Due Diligence Obligations in International Human Rights Law* (Cambridge: Cambridge University Press 2021), 113.

89 If a state directs a harmful act or exercises effective control over it, the act is considered an act of a state and thereby attributed to it under art. 8 ARSIWA, 2001 (n. 16), commentaries to art. 8, p. 47, para. 4.

90 The vast majority of international legal scholars allocates due diligence as a standard of conduct on the primary rule level, see ARSIWA, 2001 (n. 16), commentary to art. 2, p. 34, para. 3: 'Whether responsibility is "objective" or "subjective" in this sense depends on (…) the content of the primary obligation in question. The articles lay down no general rule in that regard. The same is true of other standards, whether they involve some degree of fault, culpability, negligence or want of due diligence. Such standards vary from one context to another for reasons which essentially relate to the object and purpose of the treaty provision or other rule giving rise to the primary obligation. Nor do the articles lay down any presumption in this regard (…)'; Anne Peters/Heike Krieger/Leonhard Kreuzer, 'Dissecting the Leitmotif of Current Accountability Debates: Due Diligence in the International Legal Order', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal*

states which have distinguished between attribution and a violation of due diligence, hereby suggesting they do not view due diligence as a secondary rule.[91]

This has important consequences: Even if a cyber operation reaches the threshold of prohibited force or prohibited intervention, the legally available countermeasures are exclusively determined in relation to a violation of the harm prevention rule, not in relation to the violation of such prohibitive rules. Hence, even if a cyber operation that a state failed to diligently prevent reaches the threshold of prohibited force an affected state is not entitled to self-defence but only to non-forcible countermeasures against the negligent state.

II. Notification requirement

If a state decides to take countermeasures against a negligent state, it needs to notify the affected state before taking countermeasures to give the responsible state the opportunity to respond.[92] The UK has argued that it is not always required to notify the state against which it takes countermeasures[93], and e.g. Norway[94] and Israel[95] have echoed this position. A lack of

Order (Oxford: Oxford University Press 2020), 1–19, at 7, 8; Anja Seibert-Fohr, 'From Complicity to Due Diligence: When Do States Incur Responsibility for Their Involvement in Serious International Wrongdoing?', *German Yearbook of International Law* 60 (2017), 667–708, at 707.

91 Germany, On the Application of International Law in Cyberspace, March 2021, p. 11.

92 ARSIWA, 2001 (n. 16), commentary to art. 52, p. 136, para. 4: 'he principle underlying the notification requirement is that, considering the exceptional nature and potentially serious consequences of countermeasures, they should not be taken before the other State is given notice of a claim and some opportunity to present a response.'

93 UK Attorney General Wright, Cyber and International Law in the 21st Century, Speech 23 May 2018: '(…) we would not agree that we are always legally obliged to give prior notification to the hostile state before taking countermeasures against it (…) it could not be right for international law to require a countermeasure to expose highly sensitive capabilities in defending the country in the cyber arena (…)'.

94 Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly Resolution A/RES/73/266, 13 July 2021, p 73, para. 5.2.

95 Roy Schondorf, Israel Ministry of Justice, Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations.

transparency for taking countermeasures however entails structural risks for the legal regime of self-help.[96] Furthermore, it is already acknowledged that in urgent cases no notification is required.[97] Hence, instead of generally dispensing with the notification requirement, it is preferable to assume that states in principle need to notify the affected state before taking countermeasures, unless an urgent case exists.[98]

III. Countermeasures against states

States are not entitled to take countermeasures against non-state actors, but only against states. As often non-state actors conduct cyber operations, this prima facie severely limits the normative pull of countermeasures. It has been argued that a state may 'hack back' against a non-state actor on the territory of another state if it notifies the territorial state about the harmful activity and the notified state remains passive and hereby violates its due diligence duty to take action against the harmful activity.[99] However, the termination of an activity does not induce the territorial state to act diligently and thus woud regularly not comply with the purpose requirement.[100] With regard to this unsatisfactory result it is to be noted that, in exceptional circumstances, a state may invoke necessity under Art. 25 ARSIWA to justify 'hack-back' operations.[101]

96 Highlighting the importance of explaining countermeasures to contribute to the stabilization of norms Sven Herpig, *Active Cyber Defense – Toward Operational Norms* (Stiftung Neue Verantwortung 2023), p. 20.

97 ARSIWA, 2001 (n. 16), commentary to art. 52, p. 136, para. 6: '(…) the injured State may take "such urgent countermeasures as are necessary to preserve its rights" even before any notification of the intention to do so.'

98 Schmitt, 'In Defense of Due Diligence' 2015 (n. 80), 79; in a similar vein Netherlands, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, Appendix, International Law in Cyberspace, p. 7.

99 Ibid.

100 Chircop, 'A Due Diligence Standard' 2018 (n. 3), 13. In a more liberal reading of the purpose requirement hacking back at least indirectly induces the territorial state to comply with its diligence obligations – namely to terminate the activity itself.

101 Lahmann Unilateral Remedies' 2020 (n. 33), 201f.

IV. The problem of collective countermeasures

A more recent discussion has evolved around the question whether states can take so-called 'collective countermeasures'. The concept of collective countermeasures refers to a scenario in which a non-injured state resorts to countermeasures against a norm-violating state.

States are so far largely mute or split whether such a right exists or should exist in cyberspace: Estonia[102], Ireland[103] and Costa Rica[104] have argued in favour and New Zealand at least seemed to acknowledge the possibility.[105] By contrast, France and Canada have argued against it.[106]

In international law it is so far only settled that collective countermeasures may be taken in response to violations of obligations owed to the international community as whole, i.e. *erga omnes* obligations.[107] It hence begs the question whether due diligence obligations under the harm prevention rule can be conceived as *erga omnes* obligations. While diverging methods for identifying *erga omnes* obligations exist such obligations are predominantly characterized by their material importance and their non-'bilateralizable' character.[108]

Focussing on these two characteristics already suffices to conclude that procedural due diligence obligations cannot be conceived as obligations *erga omnes*. The procedural due diligence obligation to take action in the case of an emergency[109] is e.g. only owed bilaterally to the state whose legal interest is affected by a malicious cyber operation but not the international

102 Kersti Kaljulaid, President of the Republic of Estonia at the opening of CyCon 2019, 29 May 2019, https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-openingof-cycon-2019/index.html.

103 Ireland, Position Paper on the Application of International Law in Cyberspace, July 2023, para. 26.

104 Open in this regard Costa Rica, Costa Rica's Position on the Application of International Law in Cyberspace, August 2023, para 15.

105 New Zealand, The Application of International Law to State Activity in Cyberspace, 1 December 2020, para. 22.

106 France, International Law Applies to Operations in Cyberspace, September 2019, p. 7; Canada, International Law Applicable in Cyberspace, April 2022, para.37.

107 ARSIWA, 2001 (n. 16), art. 48 lit. b: 'Any State other than an injured State is entitled to invoke the responsibility of another State (…) if (…) the obligation breached is owed to the international community as a whole.'

108 For an overview on methods for identifying *erga omnes* obligations Christian Tams, *Enforcing Obligations Erga Omnes in International Law* (Cambridge University Press 2009), 129.

109 On this procedural due diligence obligation in more detail see above chapter 4.C.II.

community as a whole. Furthermore, the duty to action would regularly be materially important only for the affected victim state. For such scenarios, caution regarding the concept of collective countermeasures seems warranted. Extending the possibility of collective law-enforcement beyond *erga omnes* norms[110] may have ramifications in other areas of international law. It furthermore carries a certain potential for abuse as it may enable a state which is not affected by a cyber operation to take action under the pretext of acting in the community interest or the interest of an injured state, while pursuing special interests.[111] It seems therefore more convincing that a non-injured state can only take countermeasures if the injured state has requested it to do so.[112]

By contrast, due diligence obligations regarding institutional capacity-building have a non-'bilateralizable' character. It is for example hard to conceive the due diligence obligations to establish cybercrime legislation or to protect the public core of the internet as an obligation owed to any particular state. Such due diligence obligations rather serve as a means to establish an international minimum standard and to counter the existence of cyber safe havens in which basic institutional preventive measures lack. The international community has a shared interest in the elimination of cyber safe havens.[113] It is hence plausible to conceive the international community as the rightholder of due diligence obligations regarding insti-

110 As e.g. suggested by Costa Rica, see Costa Rica, 'Costa Rica's Position' 2023 (n. 104), para. 15.

111 See on this risk of abuse of collective countermeasures Isabel Feichtner, 'Community Interest', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2007), para. 58; in general, international tribunals seem better equipped to ascertain community interests, see Eyal Benvenisti, 'Community Interests in International Adjudication', in Eyal Benvenisti/Georg Nolte (eds.), *Community Interests Across International Law* (Oxford: Oxford University Press 2018), 70–85, at 71.

112 This is e.g. the position of Canada, 'International Law Applicable in Cyberspace' 2022 (n. 106), para.37.

113 Przemysław Roguski, 'Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea?', in Taťána Jančárková/Lauri Lindström et al. (eds.), *20/20 Vision: The Next Decade* (NATO CCDCOE 2020), 25–42; highlighting the benefit of collective countermeasures due to the the interconnected nature of cyberspace Jeff Kosseff, 'Collective Countermeasures in Cyberspace', in *Notre Dame Journal of International and Comparative Law* 10 (2020), 18–39, at 39; See the reference to the collective interest in compliance with international law by New Zealand, 'International Law in Cyberspace' 2020 (n. 105), para. 22.

tutional capacity-building[114], not least because it is hard to conceive a duty without a correlative rightholder.[115]

The legal consequence of this conclusion would be that states may take collective countermeasures to enforce compliance with due diligence obligations regarding institutional capacity-building, in particular when calls for cessation under art. 30 ARSIWA – e.g. to enact cybercrime legislation or to establish an emergency response team[116] – have failed. In doing so, they are however bound by the above-mentioned strict purpose and proportionality limits.

V. The limited role of countermeasures for the enforcement of the harm prevention rule

The law of countermeasures hence provides states with the possibility to enforce the harm prevention rule. The purpose and proportionality requirements limit response options, yet leave states options in specific circumstances to pressure states for norm compliance or to take efficient measures of self-help. Whether the perceived 'need for greater tolerance of countermeasures'[117] and their potential increased relevance in the future[118] will materialize in practice remains to be seen.

More likely seems to be the scenario that norm stabilization is increased via continued engagement of states in international fora, such as in the UN OEWG or in the UN GGE, and by incentivizing ongoing dialogue on best practices, hereby leading to states' 'argumentative self-entrapment'.[119]

114 See already above chapter 3.C.III. Making this argument with regard to the obligation to protect the public core of the internet Roguski, 'Collective Countermeasures', 2020 (n. 113), 39.

115 Brunnée, 'Procedure and Substance' 2020 (n. 18), 173; ARSIWA, 2001 (n. 16), commentary to art. 2, p. 35, para. 8: 'there are no international obligations of a subject of international law which are not matched by an international right of another subject or subjects, or even of the totality of the other subjects (the international community as a whole).'

116 See above chapter 5.B.II.

117 Michael Schmitt, 'Three International Law Rules for Responding Effectively to Hostile Cyber Operations', JustSecurity, 13 July 2021, available at: https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/.

118 Hinting at this possibility Lahmann Unilateral Remedies' 2020 (n. 33), 200.

119 On the long-term 'argumentative self-entrapment' even of hypocritical statements with a minimum degree of argumentative consistency see Thomas Kleinlein, 'Cus-

Parallely, retorsive or deterrent measures – which fall outside of the scope of law enforcement in the strict sense – are likely to play a significant role.[120] The enforcement prong hence seems only partially decisive for the potential of the harm prevention rule in cyberspace.

tomary International Law and General Principles Rethinking Their Relationship', in Brian D. Lepard (ed.), *Reexamining Customary International Law* (Cambridge: Cambridge University Press 2017), 131–158, at 156.

120 On both the normative prong via norm internalization and the punitive prong via deterrence see Roguski, 'Cyber Weapons' 2021 (n. 4), 114; highlighting retorsion as an option New Zealand, 'International Law in Cyberspace' 2020 (n. 105), para. 18.

Chapter 6: General Conclusions

A. The potential of the harm prevention rule in cyberspace

This study has shown that, despite a widespread perceived lack of clarity as to the content of the harm prevention rule, legal yardsticks regarding the threshold of cyber harm and required due diligence measures have emerged and that international law in cyberspace is far from a 'lawless lacuna'.[1]

One of the key potentials of the harm prevention rule, including its due diligence requirements, is its potential to reduce cyber safe havens. While the short-term impact of enacting cybercrime legislation, establishing investigative measures or establishing a CERT may be limited, the overall stabilizing impact of such measures is likely substantial. Due to the interconnectedness of global cyberspace, global cyber security is only as strong as its weakest link. More efforts on due diligence measures of institutional capacity-building will thus incrementally strengthen global cyber resilience. In addition it will also enable the effective implementation of procedural due diligence obligations.[2]

The harm prevention rule furthermore provides a normative framework for incentivizing procedural practices which stabilize global cyberspace.[3] It may for instance incentivize states to focus on incident management capability and to establish best practice procedures. To give just one example,

1 Luke Chircop, 'A Due Diligence Standard of Attribution in Cyberspace', *International and Comparative Law Quarterly* 67 (2018), 1–26, at 11.

2 UN GGE Report 2021, para. 53: 'Having the necessary national structures and mechanisms in place to detect and mitigate ICT incidents with the potential to threaten international peace and security enables the effective implementation of this norm. (…) For example, a State wishing to request assistance from another State would benefit from knowing who to contact and the appropriate communication channel to use. A State receiving a request for assistance needs to determine, in as transparent and timely a fashion as possible and respecting the urgency and sensitivity of the request, whether it has the capabilities, capacity and resources to provide the assistance requested. States from which the assistance is requested are not expected to ensure a particular result or outcome'.

3 Highlighting the potential of procedural due diligence obligations for stabilizing cyberspace see also Samantha Besson, 'La Due Diligence en Droit International', *Recueil des Cours de l'Académie de Droit International de la Haye* 409 (2020) 153–398, at 341, para.455.

several states have reported on their measures they have undertaken or are planning to undertake to increase cyber resilience and to implement the recommendations of the reports. Armenia reported that approved and applied technical standards (e.g. ISO) to improve its cyber security, or that it had adapted its national cybercrime legislation.[4] Similarly, Belarus reported that it had 'organized and [applied] technical norms' to protect information.[5] In the UN OEWG Canada has reported extensively on its measures to comply with the norms of responsible state behaviour.[6] Such interactional practices can contribute to norm evolution, norm adherence and normative expectations.[7]

The harm prevention rule furthermore incentivizes states to increase their efforts on technical capacity-building, in particular regarding their critical infrastructure.[8] Such technical capacity-building is crucial to improve cyber resilience.[9] Simultaneously, due to its context-dependent flexibility which takes the subjective capacity of a state into account, due diligence avoids overburdening technologically lesser developed states. The standard hereby avoids the rigidity of strict precise rules[10] which may discourage participation in the development of shared understandings of the law.[11]

The harm prevention rule and its due diligence aspects furthermore provides an accountability mechanism when attribution fails.[12] In particular,

4 UN General Assembly Resolution A/RES/72/315, 11 August 2017, p.5.
5 Ibid., p. 6.
6 Canada, Canada's implementation of the 2015 GGE norms, 2019, p. 4, 5.
7 Jutta Brunnée/Stephen J. Toope, *Legitimacy and Legality in International Law* (Cambridge: Cambridge University Press 2010), 118,119.
8 On protection of critical infrastructure as a due diligence requirement see chapter 4.D.III.
9 Paris Call for Trust and Security, 12 November 2018, p. 2: 'We underline the need to enhance broad digital cooperation and increase capacity-building efforts by all actors and encourage initiatives that build user resilience and capabilities.'
10 Martha Finnemore/Duncan B. Hollis, 'Constructing Norms for Global Cybersecurity', *American Journal of International* 110 (2016), 425–478, 467: 'The chosen structure of the norm may influence chances for uptake and internalization. The precision of rules, for example, imposes a rigidity that can make them unworkable as technology or circumstances change.'
11 On the importance of developing shared understandings for the transition from social norms to practices of legality Brunnée/Toopee, 'An Interactional Account' 2010 (n. 7), 56f.
12 Japan, Basic Position of the Government of Japan on International Law Applicable to Cyber Operations, 28 May 2021, p. 6: '[D]ue diligence obligation may provide grounds for invoking the responsibility of the State from the territory of which a

specific procedural due diligence obligations to take action against harmful cyber operations, to warn about risks, or to cooperate with regard to investigations, can provide accountability mechanisms in the case of harm.[13] Beyond binding procedural measures, it moreover incentivizes states to engage in cooperative mechanisms.[14] Contrary to the attribution of an actual harmful act to a state failure to discharge due diligence requirements can usually be proven: It is for example usually possible to determine whether a state responded to a call for taking action against an ongoing cyber incident. It is also easy to determine whether a state has enacted sufficient cybercrime legislation.

An often neglected aspect is that the harm prevention rule also entails a negative prohibitive dimension.[15] The harm prevention rule hereby offers a legal tool to rein in malicious state-sponsored cyber operations while avoiding the risky conceptual ramifications of other suggestions for grasping low-level cyber harm, such as a prohibitive sovereignty rule.

Yet, it is also clear that the harm prevention rule is not a silver bullet. On the one hand, its efficiency is limited due to norm-internal aspects. On the other hand, it is limited due to general challenges of international law in cyberspace. The need for specification makes the efficiency of the rule dependent on the willingness of states to fill its content with sufficiently clear meaning. Due to the strategic ambiguity of states opinio iuris is so far only gradually evolving. As long as the content of due diligence is unclear states are likely unwilling to take more than minimal efforts to achieve compliance.[16] A culture of compliance based on the international rule of

---

cyber operation not attributable to any State originated. It is possible at least to invoke the responsibility of such a State for a breach of its due diligence obligation, even if it is difficult to prove the attribution of a cyber operation to any State.'

13 On the value of cooperation for risk mitigation see UN GGE Report 2021, para. 55: 'Where the malicious activity is emanating from a particular State's territory, its offer to provide the requested assistance and the undertaking of such assistance may help minimize damage, avoid misperceptions, reduce the risk of escalation and help restore trust.'

14 On the importance of a sophisticated network of international procedural obligations for (environmental) risk mitigation Caroline E. Foster, *Science and the Precautionary Principle in International Courts and Tribunals. Expert Evidence, Burden of Proof and Finality* (Cambridge: Cambridge University Press 2011), 7.

15 See chapter 4.A; 2.A.VI.

16 See generally Dinah L. Shelton, 'Law, Non-Law and the Problem of "Soft Law"', in Dinah L. Shelton (ed.) *Commitment and Compliance: The Role of Non-Binding Norms in the International Legal System* (Oxford: Oxford University Press 2000), 1–20, at 14.

law[17] will eventually require more specification as the flexibility of the rule may render it endlessly malleable.[18]

Furthermore, the harm prevention rule's efficiency is hampered by the Janus-faced approach of states to international law in cyberspace. The strategy of paying lip service to international law while conveniently evading commitments or limits for own cyber offensive operations risks undermining the steering force of international law.[19] The capability of international law for inducing norm-adherence is in any case challenged in cyberspace as important preconditions of cyber security lie outside of the reach of international law.

For example, a significant aspect of cyber security is cyber education. Due to persistent problems of human error, and the significant threat for social engineering any meaningful resilience strategy requires cyber-education by every individual user.[20] Contributing to this de facto expertise can however hardly legally be prescribed by international law and needs an incremental domestic approach. Due to the crucial role of technology also other normative regime gain an enormously relevant role. For example, product liability rules[21], private actor self-regulation, and technical best practice standards seem to have an equally crucial role for cyber risk

17 Chircop, 'A Due Diligence Standard' 2018 (n. 1), 11.

18 Heike Krieger/Anne Peters, 'Due Diligence and Structural Change in the International Legal Order', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 351–390, at 385.

19 François Delerue, 'Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace', in Taťána Jančárková/Lauri Lindström et al. (eds.), *Going Viral* (NATO CCDCOE 2021), 9–24, at 24: 'States appear to be turning their backs on the international rules-based order. Such an approach bears the risk of endangering the international peace and stability of cyberspace. If international law is not perfect and has not prevented breaches of peace and aggressions in the past, it constitutes a powerful tool and the best regulatory framework at our disposal if we want to avoid turning cyberspace into a new Wild West.'

20 ITU, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (ITU 2012), 18: '(…) user education should be an essential part of any anti-cybercrime strategy.'; Information and awareness campaigns may be an important tool in this regard.' Such soft skills are clearly beyond the purview of international law and even law generally.

21 On the relevance of product liability regarding critical infrastructure protection Michael Berk, 'Recommendation 13g and h', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 191–222, at 221.

mitigation as international law and overall challenges the assumption of international law as the ultimate legal regime for regulating international peace and security.

Overall, however, the significant stabilizing potential of the rule should be acknowledged. As this study has shown, due diligence standards have already emerged with regard to an international minimum standard and further standards of diligent conduct are already emerging or may emerge in the future. States are well advised to embrace this development and commit to this process by specifying their opinio iuris as to the relevant harm threshold and required measures. International law may hereby live up to its aspiration to ensure international peace and security in cyberspace.

B. Central findings

1. The harm prevention rule is a customary rule of a general character that is inherent in the structure of the international legal order. It thus applies in new areas of international law, such as cyberspace, unless state practice and opinio iuris indicates that states consider the rule inapplicable. The threshold for the applicability of the rule in a new area such as cyberspace is accordingly diminished. Deductive considerations are however aided by inductive considerations.
2. The harm prevention rule requires states to prevent significant harm to the legally protected of other states emanating from their territory or under their jurisdiction and control. It hereby provides an accountability mechanism in cases when attribution of harmful acts to a state fails.
3. The required standard of conduct to discharge the obligation of prevention is due diligence. Due diligence and harm prevention are often referenced synonymously in the international legal discourse. As due diligence as a standard of conduct plays a role in international law beyond the harm prevention rule and herein reaches to the realm of soft law, this study argues that it is preferable to refer to the 'harm prevention rule' for expressing the legal rationale ascertained inter alia in *Island of Palmas, Trail Smelter* and *Corfu Channel*.
4. Complementary to the preventive due diligence dimension the harm prevention rule also entails a negative prohibitive dimension that obliges states not only to prevent significant harm emanating from non-state actors, but also not to conduct such harmful activities themselves.

5. States have acknowledged the applicability of the harm prevention rule in cyberspace. However, uncertainty remains regarding the content of the rule, in particular, the threshold of risk of harm that triggers due diligence obligations, as well as the required diligence measures. This hampers the rule's operationability in practice.
6. Due diligence obligations are triggered by the risk of significant cyber harm. Also general or abstract risks trigger due diligence obligations to prevent. If a certain harmful act reaches the threshold of a prohibitive rule this indicates that the threshold of a risk of significant harm is met. Reaching such a threshold is however not necessary to conclude on the significance of a risk of harm. 'Mere' significance of a risk of cyber harm hence suffices to trigger due diligence obligations to prevent. An important indicator for assessing whether cyber harm is significant is whether it has become a concern in inter-state relations.
7. Cyber harm that reaches the threshold of a prohibitive rule is harm that would amount to a violation of the prohibition on the use of force, a prohibited intervention or an arguably evolving prohibitive sovereignty rule in cyberspace. The study however cautions that acknowledging a sovereignty rule in cyberspace may have negative conceptual ramifications, both in cyberspace, as well as in other areas of international law.
8. Economic cyber harm is an important further category of significant cyber harm. In particular, cyber harm to intellectual property and trade secrets, as well as the economic impact of ransomware operations on individuals, businesses, and organizations have become a concern in inter-state relations. States however still need to specify criteria for assessing different degrees of harmfulness of economic harm.
9. Cyber harm to critical infrastructure is a further category of significant harm. States diverge in their definitions of critical infrastructures but coalesce around a list of key critical infrastructures.
10. Cyber harm to the public core of the internet has been highlighted as relevant harm in the UN GGE, the UN OEWG, as well as by several states and can thus be considered significant cyber harm which states are obliged to prevent.
11. The harmfulness of cyber espionage operations has become a cross-cutting concern in international relations. In particular, espionage operations against governmental and international public institutions, mass-scale surveillance operations and economic espionage operations have emerged as espionage operations of particular concern. Criteria

for assessing the significance of cyber harm are however so far only cautiously emerging. Regarding all categories specific prohibitions as *lex specialis* may alternatively or complementarily evolve to their inclusion as significant cyber harm under the harm prevention rule.

12. The negative prohibitive dimension of the harm prevention rule obliges states not to conduct activities that cause significant cyber harm to other states. The preventive due diligence dimension requires states to take all reasonable and feasible measures which are appropriate in the specific circumstances. What is to be considered reasonable is influenced by other rules of international law, inter alia rules of international human rights law.
13. Two main categories of due diligence requirements can be discerned: Measures of institutional capacity-building and procedural measures.
    a) While procedural due diligence obligations are based on a broad normative expectation of international cooperation a general due diligence duty to cooperate is not sufficiently specified to be justiciable. It is preferable to turn to specific cooperative due diligence obligations: Due diligence obliges states to take action against imminent or ongoing cyber operations emanating from their territory. There are also strong reasons that states are obliged to warn about imminent risks of cyber harm once they are or should be aware of such risks but states are so far cautious to commit to such a duty.
    b) Due diligence also requires states to cooperate regarding criminal investigations, in particular through mutual legal assistance. In practice, a significant number of *lex specialis* exceptions, as well as slow responses, hamper the efficiency of cybercrime cooperation in practice. States are however at least obliged to provide reasons for refusals to cooperate.
    c) Due diligence requires states to address the problem of ICT vulnerabilities. States are prohibited from undermining the integrity of the supply chain themselves. *De lege ferenda* a due diligence obligation may emerge to establish vulnerabilities equities processes for weighing the utility of retaining a vulnerability against associated risks. Due to the risks of retaining a vulnerability, the presumption should be in favour of disclosure. However, only very few states have so far explicitly advocated for such a presumption. Disclosure of vulnerabilities and provision of remedies may also be required under the duty to protect under international human rights law.

d) Regarding measures of institutional capacity-building states are required to criminalize key cybercrime offences and establish key investigative measures. They however have discretion in implementing this requirement. There are strong reasons to establish criminalization exclusions for security researchers. The establishment and application of investigative measures states needs to comply with international human rights law, and in particular with the right to privacy. Human rights safeguards, such as time limits, judicial authorization, or limitation to particular offences, may be considered best practice.
e) States need to use the means of acquiring knowledge in cyberspace which they have established. States may furthermore be required to set up a basic infrastructure, via legislative and administrative measures, that brings them into the position to acquire knowledge of harmful cyber activities and to hereby keep being informed about activities on their territory.
f) States need to protect their own critical infrastructure against cyber harm. Due to likely international ramifications of cyber harm to critical infrastructure this obligation is both a requirement under international human rights law, as well as under the harm prevention rule.
g) Due diligence also requires states to set up points of contacts for international cyber incidents. Such points of contacts are an institutional prerequisite for discharging procedural due diligence obligations to take action in case of ongoing malicious cyber operations or to cooperate in cybercrime investigations. Usually, the international point of contact will be a national CERT.

14. When a state is violating a due diligence requirement state responsibility is triggered. Already mere negligence constitutes an internationally wrongful act, even without the occurrence of harm. As a consequence, the law of state responsibility is applicable, parallel to the complementary application of preventive primary rules, often also termed the 'liability' regime. In the case of harm, a violated state is entitled to compensation. Cessation may require a state to set up institutional safeguards.
15. An injured state can also resort to countermeasures. However, regularly the purpose and proportionality requirement in the law of countermeasures will limit the response of states by cyber means. States are generally required to notify a targeted state before taking countermeas-

ures. So far, states have been reluctant to resort to countermeasures and have instead turned to retorsion, deterrence and covert operations. The traditional law enforcement prong is thus of limited practical relevance with regard to the enforcement of the harm prevention rule.

16. The harm prevention rule and its due diligence aspects may become a potent tool for stabilizing global cyberspace. Norm stabilization will be increased via continued engagement of states in international fora, such as the UN OEWG or the UN GGE. By incentivizing ongoing dialogue on best practice and argumentative self-entrapment norm internalization may occur over time. A lack of clarity as to the content and application of the rule however brings the risk that states turn away from the rule.
17. The stabilizing function of the harm prevention rule and international law in cyberspace is only complementary to other legal regimes, such as product liability, technical standards, non-state actor self-regulation, as well as extra-legal factors, such as technological capacity and user education.

Bibliography

Liisi Adamson, 'Recommendation 13c', in Enekken Tikk (ed.), Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary (United Nations Office for Disarmament Affairs 2017), 49–75

Daniel Albrecht, 'Chinese Cybersecurity Law Compared to EU-NIS-Directive and German IT-Security Act', *Computer Law Review International* (2018), 1–5

Anthony d'Amato, *The Concept of Custom in International Law* (Cornell University Press, 1971)

Elif Askin, 'Economic and Social Rights, Extraterritorial Application', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2019)

Helmut Philipp Aust/Prisca Feihle, 'Due Diligence in the History of the Codification of the Law of State Responsibility', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 42–58

Helmut Philipp Aust, 'Spionage im Zeitalter von Big Data – Globale Überwachung und der Schutz der Privatsphäre im Völkerrecht', *Archiv des Völkerrechts* 52 (2014), 375–406

Björnstjern Baade, 'Due Diligence and the Duty to Protect Human Rights', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 92–108

Björnstjern Baade, 'Fake News and International Law', *European Journal of International Law* 29 (2018), 1357–1376

Björnstjern Baade, *Der Europäische Gerichtshof für Menschenrechte als Diskurswächter* (Berlin: Springer 2017)

Jelena Bäumler, *Das Schädigungsverbot im Völkerrecht* (Berlin: Springer: 2017)

Jelena Bäumler, 'Implementing the No Harm Principle in International Economic Law: A Comparison between Measure-Based Rules and Effect-Based Rules', *Journal of International Economic Law* 20 (2017), 807–828

Christopher D. Baker, 'Tolerance of International Espionage: A Functional Approach', *American University International Law Review* 19 (2003), 1091–1113

Karine Bannelier/Theodore Christakis, 'Prevention Reactions: The Role of States and Private Actors' (Paris: Les Cahiers de la Revue Défense Nationale 2017)

Karine Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations', *Baltic Yearbook of International Law* 14 (2014), 23–39

Julio Barboza, 'International Liability for the Injurious Consequences of Acts Not Prohibited by International Law and Protection of the Environment', *Recueil des Cours de l'Academie de Haye* 247 (1998), 291–406

Jens Bartelson, 'Dating Sovereignty', *International Studies Review* 20 (2018), 509–513

Giulio Bartolini, 'The Historical Roots of the Due Diligence Standard', in Heike Krieger/Anne Peters/Leonhard Kreuzer (eds.), *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 23–41

Eyal Benvenisti, 'Community Interests in International Adjudication', in Eyal Benvenisti/Georg Nolte (eds.), *Community Interests Across International Law* (Oxford: Oxford University Press 2018), 70–85

Michael Berk, 'Recommendations 13 (g) and (h)', in Eneken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 191–222

Antal Berkes, 'Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control', *Israel Law Review* 52 (2019), 197–231

Antal Berkes, 'The Standard of 'Due Diligence' as a Result of Interchange between the Law of Armed Conflict and General International Law', *Journal of Conflict & Security Law* 23 (2018), 433–460

Samantha Besson, 'La Due Diligence en Droit International', *Recueil des Cours de l'Académie de Droit International de la Haye* 409 (2020) 153–398

Samantha Besson, 'Sovereignty', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2011)

Alan E. Boyle, 'State Responsibility and International Liability for Injurious Consequences of Acts not Prohibited by International Law: A Necessary Distinction?', *International and Comparative Law Quarterly* 39 (1990), 1–26

Jordan Branch, 'What's in a Name? Metaphors and Cybersecurity', *International Organization* 75 (2021), 39–70

Dennis Broeders, *The Public Core of the Internet* (Amsterdam: Amsterdam University Press 2015)

Gary Brown/Keira Poellet, 'The Customary International Law of Cyberspace', *Strategic Studies Quarterly* 6 (2012), 126–145

Jutta Brunnée, 'Procedure and Substance in International Environmental Law', *Recueil des Cours de l'Académie de Droit International de la Haye* 405 (2020), 77–240

Jutta Brunnée/Stephen J. Toope, *Legitimacy and Legality in International Law* (Cambridge: Cambridge University Press 2010)

Russell Buchan, *Cyber Espionage and International Law* (Oxford: Hart Publishing 2018)

Russell Buchan, 'The International Legal Regulation of Cyber Espionage', in Anna Maria Osula/Henry Rõigas (eds.) *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCD COE Publications 2016), 65–86

Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', *Journal of Conflict & Security Law* 21 (2016), 429–453

Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions', *Journal of Conflict & Security Law* 17 (2012), 211–227

Els de Busser, 'Recommendation 13d', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 77–94

Christian Calliess/Ansgar Baumgarten, 'Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective', *German Law Journal* 21 (2020), 1149–1179

Simon Chesterman, 'Secret Intelligence', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2009)

Luke Chircop, 'A Due Diligence Standard of Attribution in Cyberspace', *International and Comparative Law Quarterly* 67 (2018), 1–26

Luke Chircop, 'Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0', *Melbourne Journal of International Law* 20 (2019), 349–377

Theodore Christakis/Fabien Terpan, 'EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options', *International Data Privacy Law* 11 (2021), 81–106

Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation', *Monash University Law Review* 40 (2015), 698–736

Talita de Souza Dias/Antonio Coco, *Cyber Due Diligence in International Law* (Print version: Oxford Institute for Ethics, Law and Armed Conflict 2021)

Antonio Coco/Talita de Souza Dias, '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law', *European Journal of International Law* 32 (2021), 771–805

Antonio Coco/Talita de Souza Dias/Tsvetelina van Benthem, 'Illegal: The SolarWinds Hack under International Law', *European Journal of International Law* 33 (2022), 1275–1286

Gary P. Corn/Robert Taylor, 'Sovereignty in the Age of Cyber', *AJIL Unbound* 111 (2017), 207–212

Olivier Corten, *The Law against War – The Prohibition on the Use of Force in Contemporary International Law* (Oxford: Hart 2010)

James Crawford, *Brownlie's Principles of Public International Law* (Oxford: Oxford University Press 2019)

James Crawford, *Brownlie's Principles of Public International Law*, 8th edition (Oxford: Oxford University Press 2012)

Rebecca Crootof, 'International Cybertorts: Expanding State Accountability in Cyberspace', *Cornell Law Review* 103 (2018), 565–644

Georg Dahm/Jost Delbrück/Rüdiger Wolfrum, *Völkerrecht vol 1/1 Die Grundlagen: Die Völkerrechtssubjekte* (2nd edition, Berlin: Walter de Gruyter 1989)

François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press 2020)

François Delerue, 'Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace', in Taťána Jančárková/Lauri Lindström et al. (eds.), *Going Viral* (NATO CCDCOE 2021), 9–24

Hollin Dickerson, 'Best Practices', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2010)

Oliver Dörr, 'Prohibition of Use of Force', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2019)

Julia Dornbusch, *Das Kampfführungsrecht im internationalen Cyberkrieg* (Baden-Baden: Nomos 2018)

Pierre-Marie Dupuy/Cristina Hoss, 'Trail Smelter and Terrorism: International Mechanism to Combat Transboundary Harm', in Rebecca M. Bratspies/Russell A. Miller (eds.), *Transboundary Harm in International Law: Lessons from the Trail Smelter Arbitration* (Cambridge: Cambridge University Press 2006), 225–239

Leslie-Anne Duvic-Paoli, *The Prevention Principle in International Environmental Law* (Cambridge: Cambridge University Press 2018)

Dan Efrony/Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice', *The American Journal of International Law* 112 (2018), 583–657

Isabel Feichtner, 'Community Interest', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2007)

David P. Fidler, 'Cyberspace, Terrorism and International Law', *Journal of Conflict & Security Law* 21 (2016), 475–493

Martha Finnemore/Duncan B. Hollis, 'Constructing Norms for Global Cybersecurity', *American Journal of International* 110 (2016), 425–478

Martha Finnemore/Kathryn Sikkink, 'International Norm Dynamics and Political Change', *International Organization* 52 (1998), 887–917

Caroline E. Foster, *Science and the Precautionary Principle in International Courts and Tribunals. Expert Evidence, Burden of Proof and Finality* (Cambridge: Cambridge University Press 2011)

Danielle Flonk/Markus Jachtenfuchs/Aanke S. Obendiek, 'Authority Conflicts in Internet Governance: Liberals vs. Sovereigntists?', *Global Constitutionalism* 9 (2020), 364–386

Wolfgang Friedman, *The Changing Structure of International Law* (London: Stevens 1964)

Marco Gercke, 'The Slow Wake of A Global Approach Against Cybercrime', *Computer Law Review International* 5 (2006), 140–145

Terry D. Gill, 'Non-intervention in the Cyber Context', in Katharina Ziolkowski (ed.) *Peacetime Regime for State Activities in Cyberspace* (NATO CCDCOE 2013), 217–238

Oren Gross, 'Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents', *Cornell International Law Journal* 48 (2015), 481–511

Kari Hakapää, 'Innocent Passage', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2013)

Oona Hathaway et al, 'The Law of Cyber Attack', *California Law Review* 100 (2012), 817–885

Melissa Hathaway, 'Introduction: International Engagement on Cyber V: Securing Critical Infrastructure', *Georgetown Journal of International Affairs* (2015), 3–7

Sarah Heathcote, 'State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility', in Karine Bannelier/Theodore Christakis/Sarah Heathcote (eds.), *The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case* (London et al.: Routledge 2012), 295–314

Wolf Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace', in Christian Czosseck/Rain Ottis/Katharina Ziolkowski (eds.), *International Conference on Cyber Conflict* (2012), 7–19

Caitriona Heinl, 'Recommendation para. 13i', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 223–239

Kevin Jon Heller, 'In Defense of Pure Sovereignty in Cyberspace', *International Law Studies* 97 (2021), 1432–1499

An Hertogen, 'Letting Lotus Bloom', *European Journal of International Law* 26 (2015), 901–926

Stephen C. Hicks, 'International Order and Article 38(1)(c) of the Statute of the International Court of Justice', *Suffolk Transnational Law Journal* 2 (1978), 1–42

Zine Homburger, 'Recommendation 13a', in Eneken Tikk (ed.) *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary,* (United Nations Office for Disarmament Affairs 2017), 9–25

Eric Hutchins/Michael J. Cloppert/Rohan M. Amin, 'Reconnnaisance, Weaponization, Delivery, Exploitation, Installation, Command and Control and Action on objective', in *Information Warfare & Security Research* 1 (2011), 1–14

Eric Talbot Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense', *Stanford Journal of International Law* (38) 2002, 207–240

Jason D. Jolley, 'Recommendation para. 13f', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 169–190

Jason D. Jolley, *Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law* (University of Glasgow 2017)

Christopher C. Joyner, 'Coercion', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2006)

Asaf Lubin, 'The Liberty to Spy', *Harvard International Law Journal* 61 (2020), 185–243

Jörn Axel Kämmerer, 'Comity', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2020)

Krešimir Kamber, 'Substantive and Procedural Criminal Law Protection of Human Rights in the Law of the European Convention on Human Rights', *Human Rights Law Review* 20 (2020), 75–100

Jörg Kammerhofer, 'Uncertainty in the Formal Sources of International Law: Customary International Law and Some of Its Problems', *European Journal of International Law* 15 (2004), 523–553

Menno T. Kamminga, 'Extraterritoriality', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2012)

Helen Keller, 'Friendly Relations Declaration (1970)', in Anne Peters (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2021)

Ido Kilovaty, 'The Elephant in the Room: Coercion', *AJIL Unbound* 113 (2019), 87–91

Frederic L. Kirgis, 'Custom on a Sliding Scale', *American Journal of International Law* 81 (1987), 146–151

Uta Kohl, 'Jurisdiction in Cyberspace', in Nicholas Tsagourias/Russell Buchan (eds.) *Research Handbook on International Law and Cyberspace (Cheltenham:* Edward Elgar Publishing 2015), 30–54

Jeff Kosseff, 'Collective Countermeasures in Cyberspace', in *Notre Dame Journal of International and Comparative Law* 10 (2020), 18–39

Jan Kleijssen/Pierluigi Perri, 'Cybercrime, Evidence and Territoriality: Issues and Options', in Martin Kuijer/Wouter Werner (eds.), *The Changing Nature of Territoriality in International Law* (Netherlands Yearbook of International Law 2016), 147–173

Thomas Kleinlein, 'Customary International Law and General Principles Rethinking Their Relationship', in Brian D. Lepard (ed.) *Reexamining Customary International Law* (Cambridge: Cambridge University Pres 2017), 131–158

Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton: Princeton University Press 1999)

Markus Krajewski, 'Due Diligence in International Trade Law', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 312–328

Leonhard Kreuzer, 'Sovereignty in Cyberspace – A Rule Without Content?, in Antonio Segura Serrano (ed.), *Global Cybersecurity and International Law* (London: Routledge 2024), 29–43.

Leonhard Kreuzer, 'Hobbesscher Naturzustand im Cyberspace? Enge Grenzen der Völkerrechtsdurchsetzung bei Cyberangriffen', in Ines-Jacqueline Werkner/Niklas Schörnig (eds.), *Cyberwar – die Digitalisierung der Kriegsführung* (Wiesbaden: Springer 2019), 63–86

Heike Krieger/Jonas Püschmann, 'Law-making and legitimacy in international humanitarian law', in Heike Krieger (ed.), *Law-Making and Legitimacy in International Humanitarian Law* (Cheltenham et al.: Edward Elgar 2021), 1–14

Heike Krieger/Anne Peters, 'Due Diligence and Structural Change in the International Legal Order', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 351–390

Heike Krieger, 'Conceptualizing Cyberwar, Changing the Law by Imagining Extreme Conditions?', in Thomas Eger/Stefan Oeter/Stefan Voigt (eds), *International Law and the Rule of Law under Extreme Conditions: An Economic Perspective* (Tübingen: Mohr Siebeck 2017), 195–212

Heike Krieger/Georg Nolte, 'The International Rule of Law – Rise or Decline? – Approaching Current Foundational Challenges', in Heike Krieger/Georg Nolte/Andreas Zimmermann (eds.), *The International Rule of Law: Rise or Decline?* (Oxford: Oxford University Press 2019), 3–30.

Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020)

Heike Krieger, 'Positive Verpflichtungen unter der EMRK: Unentbehrliches Element einer gemeineuropäischen Grundrechtsdogmatik, leeres Versprechen oder Grenze der Justiziabilität?', *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* 74 (2014), 187–213

Heike Krieger, 'Krieg gegen anonymous', *Archiv des Völkerrechts* 50 (2012), 1–20

Philip Kunig, 'Prohibition of Intervention', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2008)

Henning Christian Lahmann, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace', *Duke Journal of Comparative & International Law* 32 (2021), 61–107

Henning Christian Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge: Cambridge University Press 2020)

Henning Lahmann/Robin Geiß, 'Freedom and Security in Cyberspace: Non-Forcible Countermeasures and Collective Threat-Prevention', in Katharina Ziolkowski (ed.) *Peacetime Regime for State Activities in Cyberspace* (NATO CCDCOE 2013), 621–657

Laurens Lavrysen, *Human Rights in a Positive State* (Cambridge et al.: intersentia 2017)

Brian Lepard (ed.), *Re-examining Customary International Law* (Cambridge: Cambridge University Press, 2016)

Martin C. Libicki, 'Cyberspace is not a Warfighting Domain', *I/S: A Journal of Law and Policy for the Information Society* 8 (2012), 321–336

Andreas Lichter/Max Löffler/Sebastian Siegloch, 'The Long-Term Costs of Government Surveillance', *Journal of the European Economic Association* 19 (2021), 741–789

Kubo Mačák, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers ', *Leiden Journal of International Law* 30 (2017), 877–899

Ian H. Mack, *Towards Intelligent Self-Defence: Bringing Peacetime Espionage in From the Cold and Under the Rubric of the Right of Self-Defence* (Sydney Law School 2013)

Dieter Martiny, 'Mutual Legal Assistance in Civil and Commercial Matters', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2009)

Nele Matz-Lück, 'Norm Interpretation across International Regimes: Competences and Legitimacy', in Margaret A. Young (ed.), *Regime Interaction in International Law – Facing Fragmentation* (Cambridge: Cambridge University Press 2012), 201–234

Neil McDonald, 'The Role of Due Diligence in International Law', *International and Comparative Law Quarterly* 68 (2019), 1041–1054

Alexander Melnitzky, 'Defending America against Chinese Cyber Espionage Though the Use of Active Defences', *Cardozo Journal of International and Comparative Law* 20 (2012), 537–570

Nils Melzer, *Cyberwarfare and International Law* (United Nations Institute for Disarmament Research, Ideas for Peace and Security-Resources 2011)

Marko Milanovic/Michael Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations during a Pandemic', *Journal of National Security Law & Policy* 11 (2020), 247–284

Marko Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (Oxford: Oxford University Press 2011)

Alex Mills, 'Rethinking Jurisdiction in International Law', *British Yearbook of International Law* 84 (2014), 187–239

Maria Monnheimer, *Due Diligence Obligations in International Human Rights Law* (Cambridge: Cambridge University Press 2021)

Milton L. Mueller, 'Against Sovereignty in Cyberspace', *International Studies Review* 22 (2020), 779–801

Martin Ney/Andreas Zimmermann, 'Cyber-Security Beyond the Military Perspective: International Law, "Cyberspace" and the Concept of Due Diligence', *German Yearbook of International Law* 58 (2015), 51–66

Jens David Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', *Texas Law Review* (95) 2017, 1579–1598

Alice Ollino, *Due Diligence Obligations in International Law* (Cambridge: Cambridge University Press 2022)

Phoebe Okowa, 'Procedural Obligations in International Environmental Agreements', *British Yearbook of International Law* 67 (1997), 275–336

Lassa Oppenheim, *International Law. A Treatise, Vol. II, War and Neutrality* (New York/Bombay: Longmans, Green and Co. 1906)

Bernard H. Oxman, 'Jurisdiction of States', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2007)

Andreas Paulus, 'The Judge and International Custom', *Law and Practice of International Courts and Tribunals* 12 (2013), 253–265

Anne Peters/Heike Krieger/Leonhard Kreuzer, 'Due diligence: the risky risk management tool in international law', *Cambridge Journal of International Law* 9 (2020), 121–136

Anne Peters/Heike Krieger/Leonhard Kreuzer, 'Dissecting the Leitmotif of Current Accountability Debates: Due Diligence in the International Legal Order', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 1–19

Anne Peters, 'Corruption as a Violation of International Human Rights', *European Journal of International Law* 29 (2018), 1251–1287

Anne Peters, 'The Refinement of International Law: From Fragmentation to Regime Interaction and Politicization', *International Journal of Constitutional Law* 15 (2017), 671–704

Niels Petersen, 'The Role of Consent and Uncertainty in the Formation of Customary International Law', in Brian D. Lepard (ed.) *Reexamining Customary International Law* (Cambridge: Cambridge University Press 2017), 111–130

Anton Petrov, *Expert Laws of War Restating and Making Law in Expert Processes* (Cheltenham et al.: Edward Elgar 2020)

Benedikt Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace', in: Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace* (NATO CCDCOE 2013), 189–216

Mark A. Pollack/Gregory C. Shaffer, 'The Interaction of Formal and Informal International Lawmaking, in Joost Pauwelyn/Ramses A. Wessel/Jan Wouters (eds), *Informal International Lawmaking* (Oxford: Oxford University Press 2012), 241–270

Lavanya Rajamani, 'Due Diligence in International Change Law', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 163–180

Elspeth Reid, 'Liability for Dangerous Activities: A Comparative Analysis', *International Comparative Law Quarterly* 48 (1999), 731–756

August Reinisch/Markus Beham, 'Mitigating Risks: Inter-State Due Diligence Obligations in Case of Harmful Cyber Incidents and Malicious Cyber Activity – Obligations of the Transit State', *German Yearbook of International Law* 58 (2015), 101–112

Thomas Rid, *Cyber War Will Not Take Place* (Hurst 2017)

Anthea Roberts, 'Traditional and Modern Approaches to Customary International Law: A Reconciliation', *American Journal of International Law* 95 (2001) 757–791

Przemysław Roguski, 'An Inspection Regime for Cyber Weapons: A Challenge Too Far?, *AJIL Unbound* 115 (2021) 110–115

Przemysław Roguski, '*Violations of Territorial Sovereignty in Cyberspace – an Intrusion-Based Approach,*' in Dennis Broeders/Bibi van den Berg (eds*.), Governing Cyberspace: Behaviour, Power and Diplomacy* (London: Rowman & Littlefield 2020), 65–84

Przemysław Roguski, 'Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea?' in Taťána Jančárková/Lauri Lindström et al. (eds.), *20/20 Vision: The Next Decade* (NATO CCDCOE 2020), 25–42

Marco Roscini, 'Military Objectives in Cyber Warfare', in Mariarosaria Taddeo/Ludovica Glorioso (ed.), *Ethics and Policies for Cyber Operations* (NATO CCDCO 2017), 99–114

Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press 2014)

Tom Ruys, 'The Meaning of Force and the Boundaries of the Jus ad Bellum', *American Journal of International Law* 108 (2014) 159–210

Time René Salomon, 'Mutual Legal Assistance in Criminal Matters', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2013)

Barrie Sander, 'Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections', *Chinese Journal of International Law* 18 (2019), 1–56

Beth van Schaack, 'The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change', *International Law Studies* 90 (2014), 20–65

Oscar Schachter, *International Law in Theory and Practice* (Dordrecht et al.: Martinus Nijhoff 1991)

Stein Schjolberg/Solange Ghernaouti-Hélie, *A Global Treaty on Cybersecurity and Cybercrime* (2nd edition, Oslo: AiTOslo 2011)

Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press 2017)

Michael N. Schmitt/Liis Vihul, 'Respect for Sovereignty in Cyberspace', *Texas Law Review* 95 (2017), 1639–1670

Michael N. Schmitt, 'In Defense of Due Diligence in Cyberspace', *Yale Law Journal Forum* 125 (2015), 68–81

Sven-Hendrik Schulze, *Cyber-»War« – Testfall der Staatenverantwortlichkeit* (Tübingen: Mohr Siebeck 2015)

Antonio Segura-Serrano, 'The Challenge of Global Cybersecurity', in: Antonio Segura-Serrano (ed.), *Global Cybersecurity and International Law* (Routledge 2024), 1–9

Anja Seibert-Fohr, 'From Complicity to Due Diligence: When Do States Incur Responsibility for Their Involvement in Serious International Wrongdoing?', *German Yearbook of International Law* 60 (2017), 667–708

Yuval Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law', *The Law & Ethics of Human Rights* 7 (2013), 47–71

Dinah L. Shelton, 'Law, Non-Law and the Problem of "Soft Law"', in Dina L. Shelton (ed.) *Commitment and Compliance: The Role of Non-Binding Norms in the International Legal System* (Oxford: Oxford University Press 2000), 1–20

Christina Parajon Skinner, 'An International Law Response to Economic Cyber Espionage', *Connecticut Law Review* 46 (2014) 1165–1207

Matthew Sklerov, 'Solving the Dilemma of State Response to Cyberattacks', *Military Law Review* 201 (2009), 1–85

Peter Stockburger, 'From Grey Zone to Customary International Law: How Adopting the Precautionary Principle May Help Crystallize the Due Diligence Principle in Cyberspace', in Tomáš Minárik/Raik Jakschis/Lauri Lindström (eds.), *10th International Conference on Cyber Conflict CyCon X: Maximising Effects 2018* (NATO CCD COE 2018), 245–262

Vladislava Stoyanova, 'Fault, Knowledge and Risk Within the Framework of Positive Obligations under the European Convention on Human Rights', *Leiden Journal of International Law* 33 (2020), 601–620

Jamie Strawbridge, 'The Big Bluff: Obama, Cyber Economic Espionage, and the Threat of WTO Litigation', *Georgetown Journal of International Law* 47 (2016), 833–870

Milan Tahraoui, 'Surveillance des flux de données: juridiction ou compétences de l'État, des notions à refonder', in Matthias Audit/Etienne Pataut (eds.), *L'extraterritorialité* (Paris: Pedone 2020), 141–194

Stefan Talmon, 'Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion', *European Journal of International Law* 26 (2015), 417–443

Christian Tams, *Enforcing Obligations Erga Omnes in International Law* (Cambridge University Press 2009)

Attila Tanzi, 'Liability for Lawful Acts', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2010)

Hugh W.A Thirlway, *International Customary Law and Codification: An Examination of the Continuing Role of Custom in the Present Period of Codification of International Law* (Leiden: Sijthoff 1972)

Eneken Tikk, 'Introduction', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017)

Eneken Tikk/Kadri Kaska/Liis Vihul, *International Cyber Incidents – Legal Considerations* (NATO CCDCOE 2010)

Stephen Townley, 'The Rise of Risk in International Law', *Chicago Journal of International Law* 18 (2018), 594–646

Arie Trouwborst, *Precautionary Rights and Duties of States* (Leiden/Boston: Martinus Nijhoff 2006)

Nicholas Tsagourias/Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges', *European Journal of International Law* 31 (2020), 941–967

Nicholas Tsagourias, 'Recommendation 13j', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 241–264

Bobby Vedral, 'The Vulnerability of the Financial System to a Systemic Cyberattack', in Taťána Jančárková/Lauri Lindström et al. (eds.), *Going Viral* (NATO CCDCOE 2021), 95–110

Eleonora Viganò/Michele Loi/Emad Yaghmaei, 'Cybersecurity of Critical Infrastructure', in Markus Christen Bert Gordijn Michele Loi (eds.), *The Ethics of Cybersecurity* (Berlin: Springer Nature 2020), 157–178

Federica Violi, 'The Function of the Triad "Territory", "Jurisdiction", and "Control" in Due Diligence Obligations', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 75–91

Silja Vöneky, 'Analogy', in Anne Peters (ed.), Max Planck Encyclopedia for Public International Law (Oxford: Oxford University Press 2020)

Beatrice A. Walton, 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law', *Yale Law Journal* 126 (2017), 1460–1519

Sean Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention,' in Jens D. Ohlin/Kevin Govern/Claire Finkelstein, *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford: Oxford University Press 2015), 249–270

Stephan Wilske, 'Abduction', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2019)

Thomas Wischmeyer, *Informationssicherheit* (Tübingen: Mohr Siebeck 2023)

Rüdiger Wolfrum/Mirka Möldner, 'International Courts and Tribunals, Evidence', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2013)

Rüdiger Wolfrum, 'International Law of Cooperation', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2010)

Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations Under International Law* (Cambridge et al.: Intersentia 2014)

Michael Wood, 'Customary International Law and the General Principles of Law Recognized by Civilized Nations', *International Community Law Review* 21 (2019) 307–324

William Thomas Worster, 'The Inductive and Deductive Methods in Customary International Law Analysis: Traditional and Modern Approaches', *Georgetown Journal of International Law* 45 (2014), 445–521

Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs', in Roland J. Stanger (ed.), *Essays on Espionage and International Law* (Columbus: Ohio State University Press 1962)

Li Zhang, 'A Chinese Perspective on Cyber War', *International Review of the Red Cross* 94 (2012), 801–807

Zhixiong Huang/Kubo Mačák, 'Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches', *Chinese Journal of International Law* 16 (2017), 271–310

Katharina Ziolkowski, 'General Principles of International Law as Applicable in Cyberspace' in Katharina Ziolkowski (ed.) *Peacetime Regime for State Activities in Cyberspace* (NATO CCDCOE 2013), 135–188

Blogposts

Dapo Akande/Antonio Coco/Talita de Souza Dias, 'Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond', 5 January 2021, *EJIL:Talk!*, available at: https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/

Prableen Bajpai, 'The 5 Largest Economies In The World And Their Growth In 2020', *Nasdaq*, 22 January 2020, available at: https://www.nasdaq.com/articles/the-5-largest-economies-in-the-world-and-their-growth-in-2020-2020-01-22

Russell Buchan, 'Eye on the Spy: International Law, Digital Supply Chains and the SolarWinds and Microsoft Hacks', *Völkerrechtsblog,* 31 March 2021, available at: https://voelkerrechtsblog.org/de/eye-on-the-spy/

Gary Corn, 'Covert Deception, Strategic Fraud, and the Rule of Prohibited Intervention', *LawfareBlog,* 24 September 2020, available at: https://www.lawfareblog.com/covert-deception-strategic-fraud-and-rule-prohibited-intervention

Kristen Eichensehr, 'Three Questions on the WannaCry Attribution to North Korea', *JustSecurity,* 20 December 2017, available at: https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea

Tomaso Falchetta, 'The Draft UN Cybercrime Treaty Is Overbroad and Falls Short On Human Rights Protection', *JustSecurity*, 22 January 2024, available at: https://www.justsecurity.org/91318/the-draft-un-cybercrime-treaty-is-overbroad-and-falls-short-on-human-rights-protection/

Michael P. Fischerkeller, 'Current International Law Is Not an Adequate Regime for Cyberspace', *LawfareBlog,* 22 April 2021, available at: https://www.lawfareblog.com/current-international-law-not-adequate-regime-cyberspace

Jack Goldsmith, 'Self-Delusion on the Russia Hack', 18 December 2020, *The Dispatch*, available at: https://thedispatch.com/p/self-delusion-on-the-russia-hack?s=r

Oona Hathaway/Alasdair Phillips-Robins, 'COVID-19 and International Law Series: Vaccine Theft, Disinformation, the Law Governing Cyber Operations', *JustSecurity*, 4 December 2020, available at: https://www.justsecurity.org/73699/covid-19-and-international-law-series-vaccine-theft-disinformation-the-law-governing-cyber-operations/

Sven Herpig/Ari Schwartz, 'The Future of Vulnerabilities Equities Processes Around the World', *Lawfare*, 4 January 2019, available at: https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world

Leonhard Kreuzer, 'Disentangling the Cyber Security Debate', *Völkerrechtsblog*, 20 June 2018, available at: https://voelkerrechtsblog.org/de/disentangling-the-cyber-security-debate/

Heike Krieger, 'Sovereignty – an Empty Vessel?', *EJIL:Talk!*, 7 July 2020, available at: https://www.ejiltalk.org/sovereignty-an-empty-vessel/

Marko Milanovic, 'Wieder and Guarnieri v UK: A Justifiably Expansive Approach to the Extraterritorial Application of the Right to Privacy in Surveillance Cases', *EJIL:Talk!,* 21 March 2024, available at: https://www.ejiltalk.org/wieder-and-guarnieri-v-uk-a-justifiably-expansive-approach-to-the-extraterritorial-application-of-the-right-to-privacy-in-surveillance-cases/

Marko Milanovic, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa', *EJIL:Talk!,* 26 May 2021 available at: https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/

Anne Peters, 'Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part II', *Ejil:Talk!*, 4 November 2013, available at: https://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/

Mark Pomerleau, 'What is 'sovereignty' in cyberspace? Depends who you ask', *FifthDomain*, 21 November 2019, available at: https://www.c4isrnet.com/international/2019/11/21/what-is-sovereignty-in-cyberspace-depends-who-you-ask/

Przemysław Roguski, 'The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States', 11 May 2020, *JustSecurity*, available at: https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/

Michael N. Schmitt, 'Three International Law Rules for Responding Effectively to Hostile Cyber Operations', JustSecurity, 13 July 2021, available at: https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/

Michael N. Schmitt, 'The Sixth United Nations GGE and International Law in Cyberspace', *JustSecurity,* 10 June 2021, available at: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/

Michael N. Schmitt, 'Terminological Precision and International Cyber Law', *Articles of War,* 29 July 2021, available at: https://lieber.westpoint.edu/terminological-precision-international-cyber-law/

Michael N. Schmitt, 'Russia's SolarWinds Operation and International Law', *JustSecurity*, 21 December 2020, available at: https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/

Michael N. Schmitt, 'In Defense of Sovereignty in Cyberspace', *JustSecurity,* 8 May 2018, available at: https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/

Alexis Steffaro, 'Detour or Deadlock? Decoding the Suspended UN Cybercrime Treaty Negotiations', 4 March 2024, available at: https://www.centerforcybersecuritypolicy.org/insights-and-research/detour-or-deadlock-decoding-the-suspended-un-cybercrime-treaty-negotiations/

Yevgeny Vindman, 'Is the SolarWinds Cyberattack an Act of War? It Is, If the United States Says It Is', *JustSecurity*, available at: https://www.lawfareblog.com/solarwinds-cyberattack-act-war-it-if-united-states-says-it/

Research paper

Annegret Bendiek, 'Due Diligence in Cyberspace – Guidelines for International and European Cyber Policy and Cybersecurity Policy', S*tiftung Wissenschaft und Politik* – Research Paper 2016

Carme Colomina/Héctor Sanchez Margalef/Richard Youngs, 'The Impact of Disinformation on Democratic Processes and Human Rights in the World', *Study Requested by the DROI subcommittee* (European Parliament), April 2021

David P. Fidler, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies', *ASIL Insights* 17 (2013)

Sven Herpig, *Active Cyber Defense – Toward Operational Norms* (Stiftung Neue Verantwortung 2023)

Sven Herpig, *A Framework for Government Hacking in Criminal Investigations* (Stiftung Neue Verantwortung 2018)

Klaus Lenssen, '…on the Ground: An Industry Perspective', in Ingolf Pernice/Jörg Pohle (eds.), *Privacy and Cyber Security on the Books and on the Ground* (Alexander von Humboldt Institute for Internet and Society 2018), 107–110

James Lewis, 'Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats', Center for Strategic and International Studies 2002

Tambiama Madiega, 'Digital Sovereignty for Europe', *EPRS – European Parliamentary Research Service*, July 2020

Zhanna Malekos Smith/Eugenia Lostri/James A. Lewis (Project Director), McAfee, 'The Hidden Costs of Cybercrime', 9 December 2020

Tim Maurer/Robert Morgus, *Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate* (The Centre for International Governance Innovation and the Royal Institute for International Affairs 2014)

Harriet Moynihan, 'The Application of International Law to State Cyberattacks Sovereignty and Non-intervention', *Chatham House – Research Paper*, 2019

Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views', *The Hague Program for Cyber Norms, Policy Brief,* 2020

Christina Rupp/Alexandra Paulus, *Official Public Political Attribution of Cyber Operations – State of Play and Policy Option*s (Stiftung Neue Verantwortung 2023)

Stefan Talmon, 'Das Abhören des Kanzlerhandys und das Völkerrecht', *Bonn Research Papers on Public International* Law 3 (2013)

Enekken Tikk/Mika Kerttunen, 'The Alleged Demise of the UN GGE: An Autopsy and Eulogy', *Cyber Policy Institute,* 2017

Ann Valjataga, 'Tracing Opinio Juris in National Cyber Security Strategy Documents', *NATO CCDCOE 2018*, 1–18

Expert testimonies

Helmut Philipp Aust, 1. Untersuchungsausschuss der 18. Wahlperiode des Deutschen Bundestages Stellungnahme zur Sachverständigenanhörung am 5. Juni 2014

Non-legal articles/news (online)

Ronen Bergman/David M Halbfinger, 'Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks', *NYTimes*, 18 May 2021

Ronen Bergman/Rick Gladstone/Farnaz Fassihi', Blackout Hits Iran Nuclear Site in What Appears to Be Israeli Sabotage, *New York Times*, 11 April 2021

Patrick Beuth, 'Der Spionagefall des Jahres', *Der Spiegel,* 18 December 2020

Russell Brandom, 'UK Hospitals Hit with Massive Ransomware Attack', *The Verge,* 12 May 2017, available at: https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin

Gary D. Brown/Owen W. Tullos, 'On the Spectrum of Cyberspace Operations', *Small Wars Journal*, 11 December 2012, available at: https://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations

Kellen Browning, 'Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack', *New York Times,* 2 July 2021

Tom Burt, 'New Cyberattacks Targeting U.S. Elections', *MicrosoftBlog,* 10 September 2020

Adrian Croft, 'EU Threatens to Suspend Data-sharing with U.S. over Spying Reports', *Reuters,* 5 July 2013, available at: https://www.reuters.com/article/usa-security-eu-idINDEE96409F20130705

Grace Dobush, '20-year-old German Hacker Confesses in Doxxing Case', *Handelsblatt*, 1 August 2019

Ryan Dube, 'What Is Binary Code and How Does It Work?', *Lifewire,* 2 March 2022, available at: https://www.lifewire.com/what-is-binary-and-how-does-it-work-4692749

Myriam Dunn Cavelty/Jacqueline Eggenschwiler, 'Behavioral Norms in Cyberspace', *The Security Times,* February 2019

Melissa Eddy/Nicole Pelroth, 'Cyber Attack Suspected in German Woman's Death', *New York Times*, 18 September 2020,

Josh Frühliner, 'The CIA Triad: Definition, Components and Examples', *CSO Online*, 10 February 2020, available at: https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html

Alex Grigsby, 'The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased', *Council on Foreign Relations,* 15 November 2018, available at: https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased

Thomas Holt, 'What Are Software Vulnerabilities, and Why Are There so Many of Them?', *The Conversation*, 23 May 2017

Michael Knigge, 'NSA Surveillance Eroded Transatlantic Trust', *DW*, 27 December 2013, available at: https://www.dw.com/en/nsa-surveillance-eroded-transatlantic-trust/a-17311216

Meike Laaff, 'Wie eine Cyberattacke einen ganzen Landkreis lahmlegt', *ZEIT Online*, 12 July 2021

Steve Morgan, 'Cybercrime To Cost The World $10.5 Trillion Annually By 2025', 13 November 2020, available at: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Olga Pavlova, 'Putin says Russia Prepared to Extradite Cyber Criminals to US on Reciprocal Basis', *CNN,* 13 June 2021

Chad Perrin, 'The CIA Triad', *TechRepublic,* 30 June 2008, available at: https://www.techrepublic.com/article/the-cia-triad/

Ian Phillips/Vladimir Isachenkov, 'Putin: Russia Doesn't Hack but "Patriotic" Individuals Might', APNews, 1 June 2017

James Risen/Eric Lichtblau, 'How the U.S. Uses Technology to Mine More Data More Quickly', *New York Times,* 8 June 2013

Irina Rizmal, 'Cyberterrorism: What Are We (not) Talking About?', *Diplo,* 3 August 2017

Jordan Robertson/Laurence Arnold, 'Cyberwar: How Nations Attack Without Bullets or Bombs', *Washington Post*, 14 December 2020

Dan Sabbagh/Andrew Roth, 'Russian State-Sponsored Hackers Target Covid-19 Vaccine Researchers', *Guardian*, 16 July 2020

David E. Sanger/Nicole Perlroth/Eric Schmitt, *'Scope* of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit', *New York Times,* 9 September 2021

Bruce Schneier, 'Class Breaks', *Schneier on Security*, 3 January 2017

Bruce Schneier, 'Simultaneous Discovery of Vulnerabilities', *Schneier on Security*, 15 February 2016

Vladimir Soldatkin/Humeyra Pamuk, 'Biden Tells Putin Certain Cyberattacks Should be 'off-limits'', *Reuters,* 17 June 2021

Robert Sprague/Sean Valentine, 'Due Diligence', Encyclopædia Britannica, 4 October 2018.

Mehul Srivastava, 'WhatsApp voice calls used to inject Israeli spyware on phones', *Financial Times,* 14 May 2019

Friedel Taube, 'Russia-Ukraine Conflict: What Role Do Cyberattacks Play?', *Deutsche Welle*, 28 February 2022, available at: https://www.dw.com/en/russia-ukraine-conflict-what-role-do-cyberattacks-play/a-60945572.

Ian Tennant/Summer Walker, 'Cyber, Fire and Fury', *Global Initiative,* 17 March 2022, available at: https://globalinitiative.net/analysis/un-cybercrime-treaty/.

Maegan Vazquez/Allie Malloy, 'Biden Will Discuss Recent Cyber Attack on Meat Producer with Putin in Geneva', *CNN*, 2 June 2021

Kim Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', *Wired,* 3 March 2016

Unnamed: 'Pegasus: Spyware Sold to Governments 'Targets Activists'', *BBC,* 19 July 2021, available at: https://www.bbc.com/news/technology-57881364

Unnamed: 'How the Dutch Foiled Russian "Cyber-attack" on OPCW', *BBC,* 4 October 2018, available at: https://www.bbc.com/news/world-europe-45747472

Table of Cases

Awards

Alabama Claims of the United States of America against Great Britain, Award of 14 September 1872, UNRIAA, vol. XXIX, 129

General Claims Commission (Mexico-USA), Janes, 16 November 1925, UNRIAA, vol. IV, 87.

General Claims Commission (Mexico-USA), Neer, 15 October 1926, UNRIAA, vol. IV, 62

Island of Palmas Case (Netherlands v. United States of America), Award of 4 April 1928, PCA Case No. 1925–01, p. 9, Vol. II, p. 829

Mexico-US General Claims Commission, L. F. H. Neer and Pauline Neer (USA v. United Mexican States), 15 October 1926, UNRIAA, vol. IV, 60

Permanent Court of Arbitration, South China Sea Arbitration, Philippines v. China, Award of 12 July 2016, PCA Case No 2013–19, ICGJ

Settlement of Claim Between Canada and the Union of Soviet Socialist Republics for Damage Caused by "Cosmos 954," Canada-U.S.S.R., 2 April 1981

Trail Smelter Case (United States v. Canada), Decisions of 16 April 1938 and 11 March 1941, vol. III, UNRIAA, 1905–1982

Domestic courts

BVerfG, Judgment of the First Senate of 19 May 2020, 1 BvR 2835/17

US Supreme Court, *United States v. Arjona*, 7 March 1887, 120 U.S. Reports 1887, 484

PCIJ, *The Case of the S.S. Lotus (France v. Turkey)*, Judgment of 7 September 1927, Series A, No. 10

ECtHR

ECtHR, *Case of Barbulescu v Romania*, Grand Chamber Judgment of 5 September 2017, Application no. 61496/08

ECHR, *Case of Big Brother Watch and Others v the United Kingdom,* Grand Chamber Judgment of 25 May 2021, Applications nos. 58170/13, 62322/14 and 24960/15

ECtHR, *Case of Budayeva and Others v. Russia*, Judgment of 20 March 2008, Application Nos 15339/02 et al.

ECHR, *Case of Denisov v. Ukraine,* Grand Chamber Judgment of 25 September 2018, Application no.76639/11

ECtHR, *Case of Güzelyurtlu and Others v. Cyprus and Turkey*, Grand Chamber Judgment of 29 January 2019, Application no. 36925/07

ECtHR, *Case of Kilic v. Turkey,* Judgment of 28 March 2000, Application no. 22492/93

IACtHR

ICJ

PCIJ