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.