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 1.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 1.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.