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

A. General Criteria

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

I. Risk of significant cyber harm

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

24 Ibid.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

III. Interpretation of risk of significant harm in cyberspace

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

59 See above chapter 2.D.V.

60 See chapter 1.C.

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

72 See chapter I.C.I, II.

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

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

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

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

VI. Context-dependent flexible assessment of significant cyber harm

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

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

B. Acts reaching the threshold of prohibitive rules

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

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

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

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

I. Prohibition on the use of force

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Acts amounting to a use of force in cyberspace

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

3. Application of the threshold to specific cyber incidents

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

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

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

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

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

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

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

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

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

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

117 See Introduction.

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

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

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

II. Prohibition of intervention

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

1. Recognition of the prohibition of intervention in cyberspace

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Domaine réservé

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

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

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

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

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

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

3. The challenge of asserting coercion in cyberspace

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

---

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

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

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

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

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

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

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

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

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

140 See chapter 1.C.I, II.

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

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

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

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

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

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

3.1 Interference with elections

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

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

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

146 Ibid.

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

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

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

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

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

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

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

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

3.2 Intervention in the fundamental operation of parliament

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

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

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

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

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

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

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

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

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

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

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

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

3.3 Cyber operations against critical infrastructure

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

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

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

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

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

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

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

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

3.4 Impacts on the stability of the financial system

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

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

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

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

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

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

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

---

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

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

171 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 118. 'Thus, if a state-sponsored cyberattack is directed at a single commercial entity such as a private bank (…) this would not engage the state's inherently sovereign functions because it is a private entity rather than a whole sector falling exclusively within the government's powers'.

172 Bobby Vedral, 'The Vulnerability of the Financial System to a Systemic Cyberattack', in in Taťána Jančárková/Lauri Lindström et al. (eds.), *Going Viral* (NATO CCDCOE 2021), 95–110.

173 On the basis that it targeted an entire financial sector Moynihan, 'The Application of International Law' 2019 (n. 58), para. 118.

174 See below chapter 3.C.I.

3.5 Harm to the political and/or cultural system

The choice of a cultural system falls within the domaine réservé. In this vein, France has also broadly referred to 'harm to political and cultural systems' as potential violations of the prohibition of intervention.[175] Open-ended references to cultural systems were also made by Iran[176] or in the joint statement by Russia and China of 2016 which refers to 'disruption of social order, incitement of inter-ethnic, inter-racial and inter-religious antagonism'[177] as potential cyber-induced prohibited interference. While the reference to interference somewhat resonates the *Nicaragua* dictum referring to the choice of 'political and cultural systems', such assertions seem dangerously indeterminate and are likely to be abused without legal specification. As noted in the context of influence operations, extensively interpreting content as harmful may incentivize undue restriction of free speech.[178] Asserting content harm as significant harm triggering due diligence obligations will regularly require close legal scrutiny.

3.6 Undermining the territorial state's exclusive right to enforce the law

In the context of the prohibition of intervention also so-called 'hack-back' operations need to be considered. Via 'hack-back' operations both state and non-state actors on the territory of a third state may aim to disable malicious cyber operations which emanate from another state's territory, e.g. by disabling a server used for an attack.[179] Such hack-back or 'active

175 France, 'International Law in Cyberspace' 2019 (n. 94), p. 7: 'Interference by digital means in the internal or external affairs of France, i.e. interference which causes or may cause harm to France's political, economic, social and cultural system, may constitute a violation of the principle of non-intervention'.

176 Iran, 'Declaration' 2020 (n. 106), Art. III, para. 2: 'Armed intervention and all other forms of intervention or attempt to threaten against the personality of state or political, economic, social, and cultural organs of it through cyber and any other tools are regarded as unlawful.'

177 The Joint Statement Between the Presidents of the People's Republic of China and the Russian Federation on Cooperation in Information Space Development, 26 June 2016, para. 2.

178 See above chapter 3.B.II.2.3.1.

179 In the context of ransomware attacks emanating from Russia US President Biden was asked whether it 'made sense to attack the actual servers that are used in an attack'. He answered in the affirmative, Remarks by President Biden Before Air Force One Departure, 9 July 2021, available at: https://www.whitehouse.gov/briefin

cyber defence'[180] operations can arguably be seen as equivalent to a law enforcement operations. As law enforcement is the exclusive right of a sovereign state and hereby falls into the domaine réservé this raises the question whether such acts reach the threshold of prohibited intervention. The Tallinn Manual rejects that extraterritorial law enforcement violates the prohibition of intervention on the grounds that it is not coercive as an affected state is not 'compelled to act in an involuntary manner or involuntarily refrain from acting in a particular way'.[181] Under the traditional approaches to coercion – e.g. requiring that a state's will is bent or that it is forced to make a policy choice it would otherwise not have taken – extraterritorial law enforcement is indeed hard to grasp as prohibited intervention. If one defines coercion more broadly, e.g. like Australia, as the effective deprivation of the ability to control, decide upon or govern matters of an inherently sovereign nature[182], arguably, hack-back operation by both state or non-state actors would deprive the territorial state of the exclusive right of law enforcement as the territorial state is not able anymore to disable the server itself (or to deliberately choose not to do so). In this reading law enforcement operations, e.g. via so-called hack-back operations, may be considered a violation of the prohibition of intervention. A cyber operation based on Art. 37 of the Swiss Intelligence Law that allows the penetration of servers located abroad to interfere with data in case of attacks against Swiss critical infrastructure[183] would then amount to a prohibited intervention. However, more opinio iuris would be required to determine under which precise conditions extraterritorial enforcement measures by both state and non-state actors reach the threshold of prohibited intervention.[184]

---

g-room/speeches-remarks/2021/07/09/remarks-by-president-biden-before-air-force-one-departure-5/.

180 UK National Cyber Security Strategy 2016–2021, p. 18.

181 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 4, p. 24, para. 22.

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

183 Switzerland, Bundesnachrichtendienstgesetz 2017, AS 2017 4095, art. 37 (1): 'Werden Computersysteme und Computernetzwerke, die sich im Ausland befinden, für Angriffe auf kritische Infrastrukturen in der Schweiz verwendet, so kann der NDB in diese Computersysteme und Computernetzwerke eindringen, um den Zugang zu Informationen zu stören, zu verhindern oder zu verlangsamen. Der Bundesrat entscheidet über die Durchführung einer solchen Massnahme (…)'.

184 On extraterritorial enforcement measures as a violation of sovereignty see in the following 3.B.II.2.3.6.

4. Lack of clarity regarding the threshold of prohibited intervention

Overall, the case study reveals a certain degree of uncertainty about the question which cyber operations reach the threshold of prohibited intervention. It is thus no surprise that statements of states on the subject matter persistently call for more clarity on what constitutes an intervention.[185] As with potential violations of the use of force even in cases when a cyber operation arguably violated the prohibition of intervention states have mostly refrained from calling out a violation.[186] Coercion regularly requires contextual factors, such as a geopolitical conflict or indicators regarding the operation's perpetrators. The problem of attributing cyber operations and the ensuing lack of clarity over an attacker's intention however frequently make the assessment of a coercive impact difficult. States are well advised to specify requirements and to highlight particular acts instead of referring to abstract criteria.[187] If a cyber operation reaches the threshold of prohibited intervention the threshold of a risk of significant cyber harm is met, hereby triggering due diligence obligations to prevent.

III. Sovereignty

A further prominent prohibitive rule may be an arguably emerging prohibitive sovereignty rule in cyberspace.

1. The suggestion of a sovereignty rule in cyberspace

The proposition of a sovereignty rule in cyberspace was first put forward by the Tallinn Manual. To address the problem of low-level cyber harm the Tallinn Manual asserted that sovereignty is not only a principle of international law from which distinct primary rules can be derived but a prohibitive primary rule itself:

> 'A State must not conduct cyber operations that violate the sovereignty of another State.'[188]

185 Netherlands, 'International Law in Cyberspace' 2019 (n. 15), p. 3.
186 Efrony/Shany, 'A Rule Book on the Shelf' 2018 (n. 118), 654.
187 See also Germany, 'Application of International Law' 2021 (n. 68), p.6.
188 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), Rule 4.

According to this position, sovereignty hence imposes an obligation on other states not to violate the sovereignty of other states via cyber operations.[189] The suggestion of a sovereignty rule in cyberspace has gained significant momentum among states and scholars.[190] During the last years a significant number of states has opined that sovereignty is a rule of international law applicable in cyberspace, including France[191], the Netherlands[192], Germany[193], Bolivia[194], the Czech Republic[195], New Zealand[196], Japan[197], Iran[198] and the member states of the AU.[199] Other states, such as the US or Israel, have avoided taking a stance[200], potentially employing a 'wait and see' strategy.[201] Only the UK has openly rejected a sovereignty rule in cyberspace.[202] This development suggests that regardless of whether in international law a sovereignty rule exists states have started to embrace such a rule in cyberspace.

189 See the definition of primary Michael Schmitt/Liis Vihul, 'Respect for Sovereignty in Cyberspace', *Texas Law Review* 95 (2017), 1639–1670, Fn. 12: 'Primary rules are those which impose either obligations or prohibitions on States.'

190 See Russell Buchan, *Cyber Espionage and International Law* (Oxford: Hart Publishing 2018), p. 11; François Delerue, 'Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace', in Taťána Jančárková/Lauri Lindström et al. (eds.), *Going Viral* (NATO CCDCOE 2021), 9–24; Kevin Jon Heller, 'In Defense of Pure Sovereignty in Cyberspace', *International Law Studies* 97 (2021), 1432–1499; critical of a sovereignty rule in cyberspace: Gary P. Corn/Robert Taylor, 'Sovereignty in the Age of Cyber', *AJIL Unbound* 111 (2017), 207–212; Oona Hathaway/Alasdair Phillips-Robins, 'COVID-19 and International Law Series: Vaccine Theft, Disinformation, the Law Governing Cyber Operations', *JustSecurity*, 4 December 2020, available at: https://www.justsecurity.org/73699/covid-19-and-international-law-series-vaccine-theft-disinformation-the-law-governing-cyber-operations/.

191 France, 'International Law in Cyberspace' 2019 (n. 94), p. 7.

192 Netherlands, 'International Law in Cyberspace' 2019 (n. 15), p. 2.

193 Germany, 'Application of International Law' 2021 (n. 68), p. 3.

194 OAS, 'Improving Transparency – 4th Report' 2020 (n. 84), para. 52.

195 Czech Republic, Statement by Mr. Richard Kadlčák Special Envoy for Cyberspace Director of Cybersecurity Department in the UN OEWG, 11 February 2020, p. 2, 3.

196 New Zealand, The Application of International Law to State Activity in Cyberspace, 1 December 2020, para. 12.

197 Japan, 'International Law Applicable to Cyber Operations' 2021 (n. 83), p. 2, 3.

198 Iran, 'Declaration' 2020 (n. 106), Art. II, para. 4.

199 AU, 'Common African Position' 2024 (n. 105), para. 13.

200 Schondorf, 'Israel's Perspective' 2020 (n. 149); Ney, 'Remarks Cyber Command' 2020 (n. 150).

201 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 23.

202 UK AG Wright, 'Cyber and International Law' 2018 (n. 103); UK Attorney General Braverman, 'International Law in Future Frontiers', Speech 19 May 2022.

2. Sovereignty as a fundamental principle of international law

The predominant understanding of sovereignty in international law is that sovereignty is a 'pivotal'[203] or fundamental[204] principle of international law from which other international legal norms derive. In the words of the ICJ the 'whole of international law rests [upon it]'.[205] Due to its generality and malleability sovereignty can hardly be defined abstractly in a succinct way. *Crawford* has highlighted that the term is 'susceptible to multiple meanings and rather a catch-all term to the collection of rights held by a state'.[206] Similarly, *Besson* asserted that '[what] sovereignty is (…) [is] determined by the rules of the international legal order'.[207] For example, the prohibition on the use of force and intervention, or jurisdictional rights derive from the principle of sovereignty.[208] Due to this dependency on *distinct* primary rules sovereignty has been described as lacking an intrinsic value[209], an 'opaque notion'[210], or even 'organized hypocrisy'.[211] Under the traditional understanding sovereignty is 'not to be equated with any substantive right'[212] but rather descriptive. It is frequently also invoked in political statements, e.g. for identity claims, without implying legal ramifications.[213] From a legal perspective, 'blunt' or 'sweeping' references to sovereignty are therefore best avoided.[214]

Due to the lack of an intrinsic value or a normative core, the traditional understanding of sovereignty is hence that it is determined by rules of international law but not a primary rule on its own – commentators have

203 Samantha Besson, 'Sovereignty', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2011), para. 1.
204 ICJ, 'Nicaragua' (n. 89), para. 263.
205 Ibid.
206 James Crawford, *Brownlie's Principles of Public International Law* (Oxford: Oxford University Press 2019), 432.
207 Besson, 'Sovereignty' (n.203), para. 109.
208 Netherlands, 'International Law in Cyberspace' 2019 (n. 15), p. 1.
209 Besson, 'Sovereignty' (n.203), para. 109.
210 Heike Krieger, 'Sovereignty – an Empty Vessel?', *EJIL:Talk!*, 7 July 2020, available at: https://www.ejiltalk.org/sovereignty-an-empty-vessel/.
211 Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton: Princeton University Press 1999).
212 Crawford, 'Brownlie's Principles' 2019 (n. 206), 432.
213 Schmitt/Vihul, 'Respect for Sovereignty in Cyberspace' 2017 (n. 189), 1656.
214 Krieger, 'Sovereignty' 2020 (n.210).

called this position the 'sovereignty-as-a-principle-only' approach.[215] This more traditional understanding of sovereignty seems to underlie para. 28 lit. b of the UN GGE Report 2015:

> 'State sovereignty and international norms and principles *that flow from sovereignty* (emphasis added) apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.'[216]

The suggestion of an autonomous sovereignty rule in cyberspace is hence prima facie atypical in international law.

3. 'Violations of sovereignty' in international practice

The editors of the Tallinn Manual and commentators supporting a sovereignty rule have however rightly pointed out that in international legal practice 'violations of sovereignty' have frequently been asserted by states and courts.[217] It is worth taking a closer look at the core of the claims of a violation of sovereignty:

In the *Cosmos 954*[218] and the *ICJ Nuclear Activities*[219] cases violations of sovereignty were based on the occurrence of physical harm. As a specific prohibition on causing significant physical harm exists – the customary obligation not to cause and to prevent significant transboundary harm[220] – the assertions of 'violations of sovereignty' in these cases appear as an argumentative short-cut for referring to interferences with the right to terri-

215 Michael N. Schmitt, 'In Defense of Sovereigtny in Cyberspace', *JustSecurity,* 8 May 2018, available at: https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/.

216 UN GGE Report 2015, para. 28b; UN GGE Report 2021, para. 71 lit. b.

217 Schmitt/Vihul, 'Respect for Sovereignty in Cyberspace' 2017 (n. 189), 1650f.; Luke Chircop, 'Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0', *Melbourne Journal of International Law* 20 (2019), 349–377.

218 *Settlement of Claim Between Canada and the Union of Soviet Socialist Republics for Damage Caused by "Cosmos 954," Canada-U.S.S.R.*, 2 April 1981, para. 17.

219 Application, Nuclear Tests (*Australia v France*), 9 May 1973 ICJ Pleadings 1, para. 3 (ii).

220 ICJ, 'Corfu Channel Case' (n.39), p.22; 'Trail Smelter' (n. 3), 1965; in the reading of this study the harm prevention rule, see chapter 2.B.

torial integrity.[221] It likely would have required more argumentative efforts to assert that the threshold of significant harm was reached or to argue for the customary applicability of the rule in the specific case.

Violations of sovereignty have also been asserted with regard to 'trespassing' cases in which physical incursions into a national airspace or the territorial sea of a state occurred, such as the *Cosmos954* or the *Corfu Channel* cases. In the *Corfu Channel* case the UK had violated Albanian sovereignty by entering the Albanian territorial sea for a minesweeping operation with warships without Albania's consent.[222] In the *Cosmos954* case the Canadian government also argued that, apart from the causation of physical harm, already the trespassing into its airspace constituted a violation of its sovereignty.[223]

Physical incursions into territory can be violations of sovereignty because they affect the territorial integrity of the territorial state. The area-specific rules on incursions by land, air or sea allow for differing levels of incursions. In the law of the sea, rights to access of landlocked countries[224] and rights to innocent passage exist.[225] Also with regard to the regulation of airspace, the content of sovereignty is spelled out in a system of primary rules.[226] While some commentators seem to assume an absolute prohibition against *any* incursion, subject to exceptions[227], the law of the sea example rather suggests that a universal rule regarding physical incursions applying to all areas of the law cannot be presumed.[228]

---

221 In a similar vein, Lahmann describes invocations of sovereignty violations in international practice as mere 'signifier[s] of [a] legally protected interest', not to be confused with the assertion of a prohibitive sovereignty rule, see Henning Christian Lahmann, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace', *Duke Journal of Comparative & International Law* 32 (2021), 61–107, at 95.

222 ICJ, 'Corfu Channel Case' (n.39), p. 36.

223 'Settlement Cosmos954' (n. 218), para. 21.

224 United Nations Convention on the Law of the Sea, 10 December 1982, 1833 UNTS 3, art. 125.

225 Ibid., art. 19; at the time of the *Corfu Channel* case such a right was customarily recognized, see Kari Hakapää, 'Innocent Passage', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2013), para. 2.

226 Chicago Convention on International Civil Aviation, 7 December 1944, 15 UNTS.

227 Heller, 'Pure Sovereignty' 2021 (n. 190), 1458, 1459; Schmitt/Vihul, 'Respect for Sovereignty in Cyberspace' 2017 (n. 189), 1645.

228 See also Gary P. Corn/Robert Taylor, 'Sovereignty in the Age of Cyber', AJIL Unbound 111 (2017), 207–212, at 210; eventually also Schmitt/Vihul do not assume such an absolute prohibition against trespass in cyberspace as they call for identification

Further examples of violations of sovereignty include kidnapping cases – e.g. the abduction of Adolf Eichmann by Israel in Argentina.[229] Abduction both affect the right to territorial integrity and the exclusive right of the territorial state to exercise (enforcement) jurisdiction in its territory.[230]

Remarkably, regarding all these cases it was hence necessary to assess whether rights derived from sovereignty, such as the right to territorial integrity or jurisdictional rights, have been interfered with in order to conclude on a violation of sovereignty. This suggests that sovereignty as such does not stipulate a sufficiently precise prohibitive rule but that the content of sovereignty and correlative prohibitions need to be spelled out in a context-specific manner via reference to primary rules derived from sovereignty but not identical with it.

4. Concepts of sovereignty in cyberspace

Due to the lack of an inherent self-ascertainable content of sovereignty it is the core question whether states have specified the meaning of a potential sovereignty rule in cyberspace. Before turning to suggestions as to the legal content of a sovereignty rule it is necessary to examine how sovereignty in cyberspace has been defined by states conceptually.

Some commentators have noted that it 'depends who you ask what sovereignty in cyberspace is'.[231] Many Western, as well as several American states, merely explain sovereignty in cyberspace as their exclusive right to regulate information and communication technology (ICT) and persons conduct-

of criteria for what constitutes a violation of territorial sovereignty – such identification of criteria would be superfluous if indeed an absolute prohibition against *any* trespass existed, see Schmitt/Vihul, 'Respect for Sovereignty in Cyberspace' 2017 (n. 189), 1647: 'The pressing task is (…) to identify the criteria for violation [of territorial sovereignty] by means of cyber operations'.

229 United Nations, Security Council, Resolution, S/Res/138, 23 June 1960.

230 Stephan Wilske, 'Abduction', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (2019), para. 12; Menno T. Kamminga, 'Extraterritoriality', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2012), para. 23.

231 Mark Pomerleau, ‚What is 'sovereignty' in cyberspace? Depends who you ask', *FifthDomain*, 21 November 2019, available at: https://www.fifthdomain.com/international/2019/11/21/what-is-sovereignty-in-cyberspace-depends-who-you-ask/.

ing cyber activities within their territory.[232] The EU has advanced the concept of European 'technological sovereignty'[233] which does not refer to an overarching legal concept but to a policy concept of strategic autonomy striving to secure European autonomy from foreign technology and service providers in a technical and economic dimension.[234] By contrast, a more elaborate concept of sovereignty in cyberspace was promoted by China in the SCO. A 2011 Draft Code of Conduct asserted 'policy authority for Internet-related public issues' as 'the sovereign right of States'. In particular, it asserted the right to 'protect (…) information space'.[235] As can be seen in lit. c of the Code of Conduct which addresses cooperation to '[curb] dissemination that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment', this information space protection includes inter alia tighter content control in cyberspace.[236] Sovereignty in this regard hence emphasizes the centrality of the state in the regulation of cyberspace, including the regulation of content in cyberspace. In China such control occurs through the so-called 'great firewall'.[237] This conception of sovereignty has implications for the question of internet governance and which level of regulatory control over routing of internet traffic and content

232 OAS, 'Improving Transparency – 4th Report' 2020 (n. 84), para. 51, p. 18; Germany, 'Application of International Law' 2021 (n. 68), p. 3.

233 EU Commission President von der Leyen, 'Shaping Europe's digital future: op-ed by Ursula von der Leyen, President of the European Commission', 19 February 2020; Also the term digital sovereignty is often used, see Tambiama Madiega, 'Digital Sovereignty for Europe', *EPRS – European Parliamentary Research Service*, July 2020.

234 Julia Pohle/Thorsten Thiel, 'Digital sovereignty', *Internet Policy Review* 9 (2020), 1–19, 10.

235 UN General Assembly, International Code of Conduct for Information Security, Annex to the Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, Developments in the field of information and telecommunications in the context of international security, A/66/359, 14 September 2011, lit. e.

236 Reiterating the official stance of the Chinese state Wuhan University/China Institute of Contemporary International Relations/Shanghai Academy of Social Sciences, Sovereignty in Cyberspace: Theory and Practice, p. 3: '[A] state enjoys (…) sovereignty, over cyber infrastructure, entities, behavior as well as relevant data and information in its territory'; Moynihan, 'The Application of International Law' 2019 (n. 58), para. 44.

237 Zhixiong Huang/Kubo Mačák, 'Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches', *Chinese Journal of International Law* 16 (2017), 271–310, at 293.

control, as well as international routes for internet traffic, a state should have.[238]

Definitions of sovereignty in cyberspace hence greatly diverge and have differing consequences regarding Internet governance. When Western states refer to sovereignty in cyberspace, they likely have a very different concept in mind as e.g. countries from the SCO.[239]

5. Legal content of a prohibitive sovereignty rule in cyberspace

Against the background of these divergent concepts of sovereignty in cyberspace suggestions regarding the prohibitive content of a sovereignty rule in cyberspace have been made.

5.1 The absolutist 'pure' sovereigntist approach

The most far-reaching position was taken by France which asserts that any penetration via a digital vector or any production of effects may constitute a violation of sovereignty.[240] Such an absolutist approach to sovereignty, requiring no particular threshold, but potentially already covering mere implant of malware without any loss of functionality as a violation of sovereignty, may be called 'pure sovereigntist'.[241] A number of states have endorsed or taken positions similar to this 'pure sovereigntist' position. Iran e.g. asserted that 'any utilization of cyberspace [which] involves unlawful

238 Danielle Flonk/Markus Jachtenfuchs/Aanke S. Obendiek, 'Authority Conflicts in Internet Governance: Liberals vs. Sovereigntists?', *Global Constitutionalism* 9 (2020), 364–386, at 374; on risks for human rights see Krieger, 'Conceptualizing Cyberwar' 2014 (n. 102), 207.

239 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 170; see also OAS, Improving Transparency': International law and State Cyber Operations (Presented by professor Duncan B. Hollis), 5th Report, CJI/doc. 615/20 rev.1, 7 August 2020, p. 32, para. 45: 'one participant suggested that there may be too many meanings for the term "sovereignty" to ascribe it a rule-like status.'; Henning Christian Lahmann, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace', *Duke Journal of Comparative & International Law* 32 (2021), 61–107, at 91.

240 France, 'International Law in Cyberspace' 2019 (n. 94), p. 6.

241 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 62; Heller, 'Pure Sovereignty' 2021 (n. 190), 1458.

intrusion to the (public or private) cyber structures which is under the control of another state'[242] constitutes a violation of sovereignty. Costa Rica held that espionage operations – and hence 'mere' access operations with no tangible physical consequences – may constitute a violation of sovereignty.[243]Also the AU explicitly rejects a *de minimis* threshold for a violation of sovereignty and takes the position that any unauthorized access constitutes a violation of sovereignty.[244] Switzerland has asserted that 'state sovereignty protects ICT infrastructure on a state's territory against unauthorised intrusion or material damage'[245] which has been interpreted as leaning towards the pure sovereigntist position.[246] Also Guatemala has broadly asserted that taking 'certain information from another State's cyber realm, even when no harm [is caused] that could affect equipment' constitutes a violation of sovereignty.[247] Protests of states against the US National Security Agency (NSA) activities revealed in 2013 have also been interpreted as leaning towards a 'pure sovereigntist' approach[248] but it is not evident that protests against mass-scale surveillance activities can be interpreted as an endorsement of the pure sovereigntist approach which lets even a single penetration suffice. The purist position has also found considerable support among commentators who frequently draw an analogy between the incursion of unauthorized aeroplanes or ships – for which they assume in principle an absolute prohibition – and unauthorized cyber operations.[249]

Yet, two caveats need to be raised: The pure sovereigntist approach is concerning regarding the apparent equation of the exclusive right to territorial sovereignty with a correlative absolute prohibition against *any* form of intrusion. In an interconnected international legal order and in particular in the globally interconnected and decentralized cyberspace such an absolutist concept of sovereignty seems unfit. The idea of a sovereign 'gate' through which any data transfer needs to transit – and the fiction

242 Iran, 'Declaration' 2020 (n. 106), Art. II, para. 4.
243 Costa Rica, Costa Rica's Position on the Application of International Law in Cyberspace, August 2023, para. 22.
244 AU, 'Common African Position' 2024 (n. 105), para. 16.
245 Switzerland, Position Paper on the Application of International Law in Cyberspace, UN GGE 2019/2021, Annex, 2021, p. 2.
246 Heller, 'Pure Sovereignty' 2021 (n. 190), 1459.
247 OAS, 'Improving Transparency – 4th Report' (n. 84), 2020, para. 52.
248 Heller, 'Pure Sovereignty' 2021 (n. 190), 1460.
249 Delerue, 'The Rule of Sovereignty in Cyberspace' 2021 (n. 190), 23; Heller, 'Pure Sovereignty' 2021 (n. 190), 1467; Buchan, 'Cyber Espionage' 2018 (n. 190), 193; Chircop, 'Territorial Sovereignty' 2019 (n. 217), 21.

that a state needs to consent to any 'entry' of data into its territory[250] – would fundamentally challenge the current status of Internet governance in which the ubiquity of non-physical data allows data to seamlessly circulate globally between largely private computer systems.[251]

Furthermore, assuming an analogy between the restrictive regime of airspace control and control over the territorial sea and cyberspace is not convincing. With regard to non-physical transit of data, no border controls occur. For example, there is no water police as in the territorial sea. Unlike the monitoring of a national airspace there is also no central organization that monitors all internet traffic. Only via extensive state control over internet routing and data packaging could such 'trespass' control be approximated. Such an approach, as e.g. enacted by the Russian 'Sovereign Internet Law' from 2019 which enables increased control over data traffic via 'deep packet inspection' measures[252], or the Chinese model requiring assessment of sensitive outbound data[253], essentially contradicts the governance model in particular of Western states and raises several human rights concerns, e.g. regarding freedom of information. Even if proponents of the 'pure' sovereigntist approach do not argue that state are legally entitled to such 'trespass' control, deriving an absolute prohibitive rule against *any* cyber intrusion at least makes claims of the 'sovereigntist' camp plausible that push towards granting states more regulatory control and increased access over routing of internet traffic.[254]

Furthermore, it is telling that the very same states which endorse a pure sovereigntist approach openly resort to offensive operations on the territory of other states. France notably asserts that it would use offensive cyber weapons which aim at 'neutralization of enemy systems' and 'denying

250 Arguably in this direction Russell Buchan, 'Eye on the Spy: International Law, Digital Supply Chains and the SolarWinds and Microsoft Hacks', *Völkerrechtsblog,* 31 March 2021, available at: https://voelkerrechtsblog.org/de/eye-on-the-spy/ 'If this is the case, why does a State's inherently governmental function to decide who enters its sovereign *physical* territory deserve more protection than its decision as to who enters its sovereign *cyber* infrastructure?'.

251 Milton L. Mueller, 'Against Sovereignty in Cyberspace', *International Studies Review* 22 (2020), 779–801, at 789.

252 Acknowledging this legal authority under the Russian law Germany Federal Government, Die menschenrechtlichen Auswirkungen von Social-Media-Zensur und Begrenzungen der Internetfreiheit, BT-Drs. 19/18902, 4 May 2020, p. 6.

253 Mueller, 'Against Sovereignty' 2020 (n. 251), 787.

254 Flonk et al, 'Liberals vs. sovereigntists?' (n. 238), 374.

the availability and confidentiality of adverse systems'.[255] In an apparent contradiction to its pure sovereigntist position it furthermore asserts that espionage as such is not unlawful in international law.[256] The Swiss law on regulation of intelligence operations expressly permits to hack into computer systems located on the territory of another state and potentially alter or delete data if this computer system is used for an attack against the critical infrastructure of Switzerland.[257] The law only requires the authorization of the Swiss government but does not foresee e.g. a prior notification or request for cooperation before the operation begins. While offensive cyber operations may be justifiable under international law, for example as countermeasures or due to necessity[258], it is noteworthy that neither of the states has explicitly conditioned the use of offensive weapons on such justifications. The fact that the very same states endorse offensive cyber operations puts at least a big question mark as to their willingness to adhere to the strict standards of the pure sovereigntist approach they seem to be arguing for. Hence, e.g. *Chircop* who supports a 'pure sovereigntist' approach has acknowledged that this approach cannot 'yet sensibly be described as a crystallised rule of customary international law'.[259]

5.2 Degree of infringement on territorial integrity

An alternative suggestion for the content of a sovereignty rule in cyberspace is the Tallinn Manual's suggestion that a violation of sovereignty may occur depending on the 'degree of infringement on territorial integrity'.[260] Unlike the pure sovereigntist approach which treats any penetration of IT unlawful, this approach focusses on an operation's effects to determine its unlawfulness[261]

255 Déclaration de Mme Florence Parly, Ministre des Armées, sur la stratégie cyber des armées, Paris, 18 January 2019; Arthur P.B. Laudrain, 'France's New Offensive Cyber Doctrine', Lawfareblog, 26 February 2019, available at: https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine.
256 France, 'International Law in Cyberspace' 2019 (n. 94), p. 4, fn. 2.
257 Switzerland, Bundesnachrichtendienstgesetz 2017, AS 2017 4095, art. 37.
258 On the strictly exceptional character of necessity see Lahmann, 'Unilateral Remedies' 2020 (n. 112), 257.
259 Chircop, 'Territorial Sovereignty' 2019 (n. 217), para. 20.
260 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), p. 20, para. 10.
261 On this effects-based approach Roguski, 'Territorial Sovereignty' 2020 (n. 133), 66.

The Tallinn Manual suggests various criteria as indicators for the category of 'degree of infringement upon territorial integrity': Physical damage, loss of functionality of a computer system, and activities below loss of functionality. It assumes that in case one of the first two criteria are fulfilled a violation of sovereignty may have occurred.[262] Regarding the third criterion – activity below loss of functionality, for instance the decelerated performance of a computer, or the alteration or deletion of data without a functional impact, – the Manual remained inconclusive.[263]

Several states have endorsed such an effects-based approach to a sovereignty violation, however without sufficiently specifying their understanding of this largely abstract category. Germany[264], the Czech Republic[265], Finland[266] and Costa Rica[267] have for example endorsed the first criterion proposed by the Tallinn Manual – physical damage. Germany has clarified that also ICT-external physical damage, e.g. resulting from the loss of functionality of ICT may be taken into account for assessing the significance of damage as long as a sufficiently close causal nexus is established.[268] Finland merely referred to 'material harm'.[269] The criteria for assessing the gravity of physical harm hence remain largely unclear. Only the Czech Republic specifically pointed at the 'death or injury to persons' and 'significant physical damage'[270] as violating sovereignty, yet such effects may even amount to a prohibited use of force. Due to the lack of specification it remains unclear which quantitative and qualitative effects physical harm would need to have to amount to a sovereignty violation. It is e.g. unclear which indirect effects would still be counted as sufficiently causally connected physical harm and which degree of physical harm would be considered 'significant'.

The second criterion proposed by the Tallinn Manual has been cautiously endorsed by a few states. Yet, with regard to specification states have so far remained largely inconclusive as well. Germany has e.g. endorsed the second criterion – loss of functionality – and asserted that negligible impairments on their own do not implicate sovereignty as a rule. It how-

262 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 4, p. 20, paras. 11–13.
263 Ibid., para. 14.
264 Germany, 'Application of International Law' 2021 (n. 68), p. 4.
265 Czech Republic, 'Statement UN OEWG' 2020 (n. 195), p. 3.
266 Finland, 'International law and cyberspace' 2020 (n. 10), p. 2.
267 Costa Rica, 'Costa Rica's Position' 2023 (n. 243), para. 20.
268 Germany, 'Application of International Law' 2021 (n. 68), p. 4.
269 Finland, 'International law and cyberspace' 2020 (n. 10), p. 2.
270 Czech Republic, 'Statement UN OEWG' 2020 (n. 195), p. 3.

ever avoided further specification.[271] Similarly, the AU asserted that loss or impairment of functionality of ICT infrastructure may amount to a violation of sovereignty[272] but also fell short of proposing further relevant criteria. Canada and Costa Rica have laudably specified that loss of functionality necessitating the repair or replacement of physical components may amount to a violation of sovereignty[273], while – according to Canada – the mere rebooting or reinstallation of an operating system would likely not suffice.[274] Yet, these specification attempts have so far been isolated and are hence insufficient to discern an emerging opinio iuris.

With regard to the third criterion – activities below loss of functionality – the picture is even more vague. Germany and Finland have highlighted that data modification may be relevant for a potential sovereignty violation but avoided taking a more explicit stance[275], while Ireland has broadly referred to 'interference with data' as a potential sovereignty violation.[276]

Hence, as also the editor of the Tallinn Manual has pointed out[277], more specification is needed to make the degree of infringement criterion operable in practice.

5.3 Interference with or usurpation of inherently governmental functions

The Tallinn Manual suggested a further category of potential sovereignty rule violations: 'Interference or usurpation of inherently governmental

271 Germany, 'Application of International Law' 2021 (n. 68), p. 4.
272 AU, Common African Position 2024 (n. 105), para. 16.
273 Canada, International Law Applicable in Cyberspace, April 2022, paras. 16, 17; Costa Rica, 'Costa Rica's Position' 2023 (n. 243).
274 Canada, International Law Applicable in Cyberspace, April 2022, paras. 16, 17.
275 Ibid.; Finland, 'International law and cyberspace' 2020 (n. 10), p. 2.
276 Ireland, Position Paper on the Application of International Law in Cyberspace, July 2023, para. 6.
277 Michael Schmitt, 'Russia's SolarWinds Operation and International Law', *JustSecurity*, 21 December 2020, available at: https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.

functions'.[278] The suggestion has been endorsed by states, such as the Netherlands[279], the Czech Republic[280], Finland[281], Costa Rica[282] and Guyana.[283]

As with the 'degree of infringement' criterion the content of this criterion is, however, largely unclear. To begin with the first element, it is unclear what an inherently governmental function is. The Tallinn refers to social services, diplomacy, taxes and law enforcement[284] but the notion of inherently governmental functions and in particular its overlap with a state's domaine réservé under the prohibition of intervention remains unclear.[285] Also what amounts to interference or usurpation is not sufficiently specified. The Czech Republic has referred to the s'significant [disruption of] the exercise of those functions, for example distributing ransomware[286]', but it is unclear whether also IT replacement in parliament following espionage operations, e.g. following the *SolarWinds* espionage operation, would amount to an interference.[287] Costa Rica has broadly referred to interferences with elections or health emergency responses as an example for a potential usurpation or interference with inherently governmental functions but it did not specify which technical effects would need to be achieved in order to assume that such an interference has taken place.[288]Tellingly, in the one clear example of a usurpation of inherently governmental functions – extraterritorial law enforcement – states seem to deliberately push the legal assessment towards a grey area. While New Zealand, Costa Rica and the member states of the AU have reiterated extraterritorial law enforcement in cyberspace as a violation of sovereign-

278 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), p. 21, para. 15; the commentaries on the suggestion notably contain hardly *any* reference to state practice or opinio iuris.
279 Netherlands, 'International Law in Cyberspace' 2019 (n. 15), p.3.
280 Czech Republic, 'Statement UN OEWG' 2020 (n. 195), p. 3.
281 Finland, 'International law and cyberspace' 2020 (n. 10), p. 2.
282 Costa Rica, 'Costa Rica's Position' 2023 (n. 243), para. 21.
283 OAS, 'Improving Transparency – 4th Report' 2020 (n. 84), p. 18, para. 52.
284 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 4, p.22, para. 16–18.
285 Ibid., p. 24, para. 22.
286 Czech Republic, 'Statement UN OEWG' 2020 (n. 195), p. 3.
287 Arguing that replacement costs may be the basis for finding a sovereignty rule violation, however based on the 'degree of infringement' criterion Michael N. Schmitt, 'Russia's SolarWinds Operation and International Law', *JustSecurity*, 21 December 2020, available at: https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.
288 Costa Rica, 'Costa Rica's Position' 2023 (n. 243), para. 21.

ty[289] the Netherlands asserted that it is unclear under which circumstances extraterritorial evidence collection without the consent of the territorial state is permitted.[290] Israel has left the question open if extraterritorial law enforcement measures constitute a violation of a potential sovereignty rule, while implicitly acknowledging that such operations take place.[291] Other states which have asserted sovereignty as a primary rule have remained conspicuously mute on the question whether extraterritorial law enforcement constitutes a violation of a sovereignty rule. Already a UN Study on Cybercrime from 2013 suggested that states indeed undertake such direct law enforcement operations which access extraterritorially stored data, even if consensual mutual legal assistance is the more frequent case.[292]

That states are even reluctant to commit to the criterion of extraterritorial law enforcement indicates states' general reluctance to endorse the abstract criterion suggested by the Tallinn Manual. One reason may be that the category of inherently governmental functions, just like the term sovereignty itself, is a highly abstract and politically charged term. States may hence be reluctant to specify their understanding of inherently governmental functions, possibly also due to potential unforeseen ramifications beyond cyberspace. Yet, it also seems emblematic for states' strategic ambiguity[293] to pay lip-service to international law but to conveniently evade legal limitations for own offensive cyber operations.

5.4 Exercise of state power

Close to the pure sovereigntist approach *Roguski* has proposed a nuanced approach by focussing on 'intrusion and interference'.[294] In his view, oper-

289 New Zealand, 'International Law in Cyberspace' 2020 (n. 196), p.2; Costa Rica, 'Costa Rica's Position' 2023 (n. 243), para. 18; AU, 'Common African Position' 2024 (n. 105), para. 15; see also UN Expert Group to Conduct a Comprehensive Study on Cybercrime, Draft Report of 27 July 2020, UNODC/CCPCJ/EG.4/2020/L.1/Add.1, para. 4.

290 Netherlands, 'International Law in Cyberspace' 2019 (n. 15), p. 2.

291 Schondorf, 'Israel's Perspective' 2020 (n. 149).

292 United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, Draft 2013, p. 133.

293 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 23.

294 Roguski, 'Territorial Sovereignty' 2020 (n. 133), 79: '[W]henever a foreign state damages, deletes, deteriorates, alters, or suppresses data stored on a computer system within the territory of another state (…) this action would be regarded as an

ations that affect the integrity of data constitute violations of sovereignty because they resemble the exercise of 'state power'. Operations that 'only' affect the confidentiality of data but not their integrity, such as e.g. phishing operations, would not be considered a violation even if they are conducted with malicious intent.[295] The focus on exercise of state power has the advantage that it mirrors the conceptual definition of sovereignty in cyberspace by Western states. As noted above in particular Western states approach sovereignty in cyberspace predominantly with a view to exclusive jurisdictional rights[296] – and hereby core elements of state power. It partially avoids the rigidity of the absolutist argument against any form of intrusion. Yet, the suggestion is close to the pure sovereigntist approach and hence faces similar concerns to the ones mentioned above. Furthermore, the question remains whether states indeed endorse the position that *any* alteration of data amounts to an exercise of state power.

5.5 Lack of sufficiently clear content of a sovereignty rule in cyberspace

Overall, the prohibitive sovereignty rule endorsed by states in cyberspace lacks a sufficiently specific content to be operable in practice.[297] In this vein, the OAS Report 2020 mentioned the concern that 'there may be too many meanings for the term "sovereignty" to ascribe it a rule-like status'.[298] While the pure sovereigntist approach provides a clear legal content, it may have the effect of plausibilizing claims for tighter state control over cyberspace, with potentially detrimental effects e.g. for freedom of information.[299] Furthermore, states have so far only partially endorsed the abstract effects-based criteria proposed by the Tallinn Manual. Even states that have endorsed the criteria have been reluctant to further specify and commit to more specific criteria.

---

exercise of state power and thus a violation of the territorial sovereignty of the targeted state.'

295 Ibid.

296 See above chapter 3.B.III.4.

297 See also Barrie Sander, 'Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections', *Chinese Journal of International Law* 18 (2019), 1–56, at 19–20.

298 OAS, 'Improving Transparency – 5th Report' 2020 (n. 239), p. 32, para. 45.

299 Leonhard Kreuzer, 'Sovereignty in Cyberspace – A Rule Without Content?, in Antonio Segura Serrano (ed.), *Global Cybersecurity and International Law* (London: Routledge 2024), 29–43, at 43.

Considering the wide endorsement of a sovereignty rule in cyberspace this result is baffling, yet is emblematic for states' Janus-faced approach to international law: On the one hand, states invoke international law, inter alia for deterrent purposes. On the other hand, they strategically avoid to commit to sufficiently precise rules for their own offensive cyber operations. Due to the potentially complex ramifications of committing to a precise legal content of a sovereignty rule it seems doubtful whether states are more willing to come forward with regard to the specification of a sovereignty rule in cyberspace in the future.

6. Assessing risks and benefits of a sovereignty rule in cyberspace

This result raises doubts about the potential and desirability of a prohibitive sovereignty rule in cyberspace. Commentators frequently assert that a central benefit of a sovereignty rule is that it may provide for the basis for taking countermeasures.[300] The lack of a sufficiently clear content of a sovereignty rule, however, directly challenges this assumption as it seems unlikely that states will invoke violations of sovereignty to justify countermeasures. The practical utility of a sovereignty rule in cyberspace as a basis for countermeasures may be questioned in two further respects: First, a sovereignty rule would still need to overcome the attribution problem.[301] In cyberspace, legal – as opposed to political – attribution is notoriously problematic.[302] Even if a malicious cyber operation is de facto state-sponsored, it is challenging to legally prove it with sufficient certainty in a

300 Schmitt/Vihul, 'Respect for Sovereignty in Cyberspace' 2017 (n. 189), 1669.

301 Acknowledging the persisting attribution problem Heller, 'Pure Sovereignty' 2021 (n. 190), 1437; highlighting that attribution is still necessary to conclude on the violation of a prohibitive sovereignty rule AU, 'Common African Position' 2024 (n. 105), para. 19.

302 On political attribution see Netherlands, 'International Law in Cyberspace' 2019 (n. 15), p. 6: '[political attribution is] a policy consideration whereby the decision is made to attribute (publicly or otherwise) a specific cyber operation to an actor without necessarily attaching legal consequences to the decision (such as taking countermeasures).' On the problems of attribution generally Lahmann, 'Unilateral Remedies' 2020 (n. 112), 109, 110; Nicholas Tsagourias/Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges', *European Journal of International Law* 31 (2020), 941–967; see also Introduction.

timely manner.[303] Furthermore, states are generally reluctant to resort to countermeasures following a cyber operation.[304] States hence lean towards a strategic sidelining of the legal regime of countermeasures, as exemplarily expressed by a US official following ransomware attacks, presumably originating from Russia, in July 2021:

> 'We're not going to telegraph what those [re]actions will be, precisely. Some will be manifest and visible, some of them may not be, but we expect those to take place in the days and weeks ahead.'

The indeterminacy of a sovereignty rule brings the risk that it is (mis)used as a highly discretionary norm for resorting to countermeasures in cases when sufficient legal criteria lack. If indeed any cyber intrusion constituted a violation of a sovereignty rule, then in principle any hacking operation would need to be considered a potential violation of sovereignty (until it is determined that non-state actors are responsible and the operation is not attributable). Such a presumed state of persistent norm violation[305] may trigger an escalatory spiral which international law is designed to prevent.

As a further downside, a sovereignty rule may embolden authoritarian and sovereigntist approaches to state control over cyberspace. It is likely that more authoritarian states will invoke a broad understanding of sovereignty[306], in particular with regard to content such states perceive as harmful.[307] The lack of clarity of what sovereignty in cyberspace entails may give authoritarian states a blueprint to invoke the concept for purposes

303 The fact that a cyber operation was launched from the territory of a state is insufficient to attribute the operation to that state, see e.g.UN GGE Report 2021, para. 71g: '[T]he Group recalls that the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State; and notes that accusations of organizing and implementing wrongful acts brought against States should be substantiated'.

304 Efrony/Shany, 'A Rule Book on the Shelf' 2018 (n. 118), 654.

305 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 61.

306 Highlighting this risk Ireland, 'Application of International Law in Cyberspace' 2023 (n. 276), para. 7; see also Moynihan, 'The Application of International Law' 2019 (n. 58), para. 62; Lahmann, 'Politics and Ideologies' 2021 (n. 239), 91.

307 Oona Hathaway/Alasdair Phillips-Robins, 'COVID-19 and International Law Series: Vaccine Theft, Disinformation, the Law Governing Cyber Operations', *JustSecurity*, 4 December 2020, available at: https://www.justsecurity.org/73699/covid-19-and-international-law-series-vaccine-theft-disinformation-the-law-governing-cyber-operations/.

undermining human rights. A sovereignty rule may hereby prove a Trojan horse for Western states, also in areas beyond cyberspace.

Therefore, overall, better arguments speak against a sovereignty rule in cyberspace. If states would, however, move towards specifying a sovereignty rule in cyberspace with sufficient clarity cyber operations that would reach the threshold of such a prohibitive norm would trigger due diligence obligations to prevent.

C. Significant cyber harm beyond acts reaching the threshold of prohibitive rules

Beyond cyber harm reaching the threshold of prohibitive international legal rules also the risk of 'mere' significant harm triggers due diligence obligations to prevent. While the notion of significant harm carries an inherent ambiguity this can also be considered a strength[308] as an aptly flexible criterion for the technologically new area of cyberspace. The broad benchmark for the significance of a risk of harm is whether it has become a 'concern in inter-state relations'[309], and by considering quantitative and qualitative criteria for assessing the degree of cyber harm.

I. Economic cyber harm as a category of significant cyber harm

One category of cyber harm that may be considered an emerging category of significant harm is economic harm. The harm prevention rule is open to include also economic damages as relevant harm. Although the ILC excluded non-physical harm from its Draft Articles on Prevention[310], Art. 2 acknowledges that harm to property can also be relevant harm.[311] That the

308 Crootof, 'International Cybertorts' 2018 (n. 9), 608: 'Indeed, as is often the case in international technological regulation, the inherent ambiguity of "significant harm" is a strength: it is a relatively tech-neutral standard that permits coherent but flexible legal development.'

309 Schmitt, 'In Defense of Due Diligence' 2015 (n. 54), 76.

310 To keep the principles more manageable, see Bäumler, 'Schädigungsverbot' 2017 (n. 2), 64f.

311 ILC Draft Articles on Prevention (n. 6), art. 2b: '"Harm" means harm caused to persons, property or the environment.'

harm prevention rule can address economic harm is also evidenced by its relevance in international finance law and international trade law.[312]

1. The problem of economic cyber harm

Economic harm can occur through a variety of malicious cyber activities. Cyber espionage can lead to theft of intellectual property or trade secrets. The manipulation of financial, corporate or customer data may have severe economic consequences for businesses and individuals, and e.g. lead to lost productivity or reputational harm.[313] Also replacement costs of infiltrated IT systems and necessary financial efforts for more cyber resilience, e.g. cyber insurance, can be considered sufficiently causally connected consequences of cyber harm.[314] In recent years the threat of ransomware attacks against businesses, which encrypt data and demand a ransom for its decryption, has increased. In July 2021, for example, about 400 supermarkets in Sweden had to close due to ransomware attacks that affected its payment and check out system.[315] While statistical assessments diverge, the threat of economic cyber harm is unanimously tremendous: Estimates range from 1 trillion[316] to 10,5 trillion USD damage annually by 2025[317] – which would

312 Bäumler, 'Schädigungsverbot' 2017 (n. 2), 122; Krajewski, 'Due Diligence in International Trade Law' 2020 (n. 66), 312–328. Beyond the harm prevention rule stipulating binding due diligence obligations also *soft law* diligence requirements for 'doing' due diligence exist in international economic law, see e.g. in international tax law; on voluntary 'doing' due diligence standards (as opposed to binding due diligence obligations) see chapter 2.B.

313 Christian Calliess/Ansgar Baumgarten, 'Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective', *German Law Journal* 21 (2020),1149–1179, at 1151.

314 McAfee, 'Economic Impact of Cybercrime— No Slowing Down', February 2018, p. 6.

315 Joe Tidy, 'Swedish Coop supermarkets shut due to US ransomware cyber-attack', *BBCNews*, 3 July 2021, available at: https://www.bbc.com/news/technology-57707530.

316 Zhanna Malekos Smith/Eugenia Lostri/James A. Lewis (Project Director), McAfee, 'The Hidden Costs of Cybercrime', 9 December 2020, p. 3.

317 Steve Morgan, 'Cybercrime To Cost The World $10.5 Trillion Annually By 2025', 13 November 2020, available at: https://cybersecurityventures.com/annual-cybercrime-report-2020/; Prableen Bajpai, 'The 5 Largest Economies In The World And Their Growth In 2020', *Nasdaq*, 22 January 2020, available at: https://www.nasdaq.com/articles/the-5-largest-economies-in-the-world-and-their-growth-in-2020-2020-01-22.

make the economic damage from cybercrime the third largest economy after the US and China if it was a country.[318] Due to the expanding attack surface that comes along with the continuously increasing social interconnectivity the economic damage from cyber harm is expected to continue to rise in the near future.[319]

2. Increasing concern about economic cyber harm

It hence comes as no surprise that states are heavily concerned about economic and financial harm caused by malicious cyber activities. The UN GGE and the UN OEWG Reports emphasized the concern about economic harm from malicious cyber activities[320] and also the Tallinn Manual acknowledged the increasing concern about economic cyber harm.[321] Also, states have made clear in protests or reactions that they consider certain forms of economic harm inacceptable in international relations. For example, the first EU Council Decision on 'restrictive measures against cyber attacks' in July 2020 was inter alia based on the fact that 'significant economic loss' had occurred.[322] The US considered the economic harm inflicted on Sony in 2014, presumably by North Korea, as 'outside the bonds of acceptable state behaviour'.[323] With regard to the persistent DDoS attacks

318 Bajpai, 'Largest Economies' 2020 (n. 318).
319 Morgan, 'Cybercrime Cost' 2020 (n. 318).
320 UN OEWG, Final Report 2021, paras. 18, 19; 'States concluded that there are potentially devastating security, economic (…) consequences of malicious ICT activities on critical infrastructure (CI) and critical information infrastructure (CII) (…) States also concluded that ICT activity contrary to obligations under international law (…) could pose a threat […to] economic development and livelihoods (…)'; UN GGE Report 2021, para. 8; UN GGE Report 2015, para. 7.
321 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 4, para. 28, 'The International Group of Experts acknowledged that States appear to be increasingly concerned about cyber operations that result in severe economic loss (…)'.
322 Council of the European Union, Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, L 246/12, Annex:'Operation Cloud Hopper" targeted information systems of multinational companies in six continents, (…) resulting in significant economic loss; (…) NotPetya" or "EternalPetya" rendered data inaccessible (…) resulting amongst others in significant economic loss.'
323 US, Federal Bureau of Investigation, Update on Sony Investigation, 19 December 2014.

on US financial institutions in 2016 the US indicted seven Iranian hackers, basing its indictment inter alia on the high remediation costs required and that the attacks sabotaged US financial institutions and undermined the integrity of fair competition.[324] France considered economic cyber harm even as a potential use of force.[325] Such a rather far-fetched interpretation would likely lead to a risk of escalation, in particular in areas outside of cyberspace. But it similarly exemplifies that the concern about economic cyber harm is pervasive.

3. Criteria for assessing the significance of economic harm

As it is clear that not every economic harm caused by cyber activities triggers due diligence duties to prevent, criteria are necessary for assessing when economic harm crosses the threshold of significance and hereby triggers due diligence duties. The difficulty of assessing economic harm makes the determination of a precise threshold of prohibited economic harm particularly complex.[326] Yet, assessing different degrees of economic harm in international law is not *per se* unfeasible. For example, in international trade law tribunals have contributed to specifying criteria for assessing the gravity of economic harm.[327]

3.1 Violation of intellectual property rights and trade secrets

An important category of significant economic cyber harm may be the degree of interference with intellectual property rights and trade secrets, and consequent harmful effects, e.g. on fair competition. Other harmful

324 US Department of Justice, 'Manhattan U.S. Attorney Announces Charges against Seven Iranians for Conducting Coordinated Campaign of Cyber Attacks against U.S. Financial Sector on Behalf of Islamic Revolutionary Guard Corps-Sponsored Entities', Press Release 24 Mach 2016.

325 France, 'International Law in Cyberspace' 2019 (n. 94), p. 8.

326 This difficulty is also reflected in the contested discussions around economic pressure or coercion as a use of force or a prohibited intervention, on this issue see Kunig, 'Prohibition of Intervention' 2008 (n. 123), para. 25.

327 Bäumler, 'Schädigungsverbot' 2017 (n. 2), 122f.

consequences may be, inter alia, the hampering of 'research, trial, manufacture, and distribution of vaccines'[328] in the health sector.

States have repeatedly pushed back against intellectual property violations via cyber means of both state and non-state actors. The EU Cyber sanction decision regarding '*Operation Ground Hopper*' and '*NotPetya*' was e.g. inter alia based on infringement of intellectual property rights, stating as a reason for the restrictive measure that 'commercially sensitive data [had been accessed without authorization]'[329], hereby reflecting Art. 3 lit. d of the EU Cyber Decision which lists theft of intellectual property as a relevant factor for determining whether a significant effect constitutes an external threat to the Union or its member states.[330] The US and the UK have protested against infringements of intellectual property on vaccine research during the COVID-pandemic[331] and also Switzerland and Germany have made clear that they consider economically motivated espionage as harmful.[332] Also, international legal scholars have highlighted the relevance of 'significant costs of targeted facilities' as relevant harm following espionage operations against intellectual property.[333]

States have furthermore aimed at reducing intellectual property violations through non-binding informal agreements. Such informal agreements and statements reflect both the positive preventive, as well as the negative prohibitive dimension. Regarding the positive preventive dimension the Western-led Paris Call for Trust and Security of 2018 e.g. called on states to prevent theft of intellectual property.[334] Reflecting the prohibitive negative

328 See ELAC, 'Oxford Statement Health Care Sector' 2020 (n. 18).

329 Council of the European Union, Decision 2020/1127 (n. 322), Annex.

330 Council of the European Union, Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 7299/19, 14 May 2019, art. 3d: 'The factors determining whether a cyber-attack has a significant effect as referred to in Article 1(1) include (…) the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property.'

331 UK, Foreign Secretary, 'UK condemns Russian Intelligence Services over vaccine cyber attacks', 16 July 2020.

332 On this stance Homburger, 'Recommendation 13a' 2017 (n. 54), para. 19; Switzerland, Submission of Switzerland to the United Nations Secretary-General's report, (A/72/315).

333 See ELAC, 'Oxford Statement Health Care Sector' 2020 (n. 18), para. 2: 'International law prohibits cyber operations by States that have significant adverse or harmful consequences for the research, trial, manufacture, and distribution of a COVID-19 vaccine, including by means (…) which impose significant costs on targeted facilities in the form of repair, shutdown, or related preventive activities'.

334 Paris Call 2018 (n. 11), p.3.

dimension of the harm prevention rule, ASEAN and the US declared in a statement that no state should 'conduct or knowingly support ICT-enabled theft of IP'[335], reiterating a similar declaration made in the MoU of 2015 between the US and China, and UK and China.[336]

A G20 statement e.g. linked protection of intellectual property to responsible state behavior (which in principle includes the harm prevention rule and its diligence aspects).[337] Additionally, several commentators have highlighted that harm to intellectual property may be considered significant harm under the harm prevention rule.[338] These developments indicate that cyber harm against intellectual property may amount to significant harm that triggers due diligence obligations to prevent.[339]

Grasping cyber harm to intellectual property as relevant harm under the harm prevention rule has an important gap-filling function: While the right to intellectual property is protected by the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) of the World Trade Organization (WTO), in particular by Art. 39 TRIPS this protection is limited. Art. 39 (1), (3) TRIPS requires states to protect undisclosed information

335 ASEAN – US Cybersecurity Cooperation, Statement, 15 November 2018: '(…) [N]o State should conduct or knowingly support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors (…)'.

336 U.S.-China Cyber Agreement, 16 October 2015, 'the United States and China agreed (…) refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property'; UK Foreign & Commonwealth Office, 'UK-China Joint Statement 2015', 22 October 2015, https://www.gov.uk/government/news/uk-china-joint-statement-2015: 'The UK and China agree not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of providing competitive advantage'; Moynihan, 'The Application of International Law' 2019 (n. 58), para. 145.

337 G20 Leaders' Communiqué, 16 November 2015, para. 26: '(…) we affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors (…) we (…) commit ourselves to the view that all states should abide by norms of responsible state behaviour in the use of ICTs'.

338 Arguing for state accountability for economic espionage based on the ICJ *Corfu Channel* rationale Christina Parajon Skinner, 'An International Law Response to Economic Cyber Espionage', *Connecticut Law Review* 46 (2014) 1165–1207, at 1192; Antonio Coco/Talita de Souza Dias/Tsvetelina van Benthem, 'Illegal: The SolarWinds Hack under International Law', *European Journal of International Law* 33 (2022), 1275–1286, at 1283.

339 In this vein Coco/Dias/van Benthem, '*The SolarWinds Hack*' 2022 (n. 338), 1283.

or data in order to prevent unfair competition.[340] The predominant understanding of Art. 39 TRIPS is however that its protective scope is limited to a state's territory.[341] Hence, in this reading, Art. 39 TRIPS neither entails a prohibition to conduct economic espionage on the territory of a third state, nor an obligation to prevent such activities emanating from a state's territory. Integrating economic cyber harm to intellectual property within the scope of the harm prevention rule would fill this gap.

The big question is whether any infiltration of intellectual property and trade secrets on another state's territory via cyber means is considered significant harm. The protests against espionage against single vaccine centres, e.g. by the UK and the US, shows that in principle also operations against a single entity may amount to a concern in inter-state relations. Yet, if any compromising of intellectual property sufficed, this would, as a consequence, lead to an extraterritorial extension of the protective scope of Art. 39 TRIPS via the harm prevention rule. As the TRIPS agreement may be considered *lex specialis* it seems more convincing to assume that the protective scope under the customary harm prevention rule is lower and that not every risk of a violation of intellectual property triggers due diligence duties to prevent. A possible approach could hence be that harmful effects of a substantial number of cyber espionage operations cumulatively amount

340 WTO, Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), 15 April 1994, Annex 1C, Marrakesh Agreement Establishing the World Trade Organization, 1869 UNTS 299, 33 ILM 1197 (1994), art. 39 (1), (3): 'In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 3. (…) In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use.' All 164 WTO member states are party to the TRIPS agreement. Protection against unfair competition was already granted by Article 10bis which prohibits acts that constitute unfair competition, Paris Convention (incorporated into TRIPS), art. 10bis.

341 David P. Fidler, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies', *ASIL Insights*, 20 March 2013, available at: www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-internationallaw-controversies-involving; Jamie Strawbridge, 'The Big Bluff: Obama, Cyber Economic Espionage, and the Threat of WTO Litigation', *Georgetown Journal of International Law* 47 (2016), 833–870; but arguing for the extraterritorial application of Art. 39.2 TRIPS and Art. 10bis Paris Convention as prohibiting economic espionage Buchan, 'Cyber Espionage' 2018 (n. 190), 133, 141.

to significant harm. Eventually, states need to be more forthcoming in their opinio iuris to clarify the threshold.

3.2 Further criteria for assessing the gravity of economic harm

In which further constellations disruptive and destructive cyber harm amounts to significant economic harm is difficult to determine. For example, under which circumstances does a ransomware operation against a business or individual constitute significant harm? State practice, opinio iuris and international legal documents provide some, yet so far ambiguous hints.

With regard to ransomware, US president Biden broadly asserted that:

> '[The] United States expects when a ransomware operation is coming from [Russia's] soil – even though it's not sponsored by the state – we expect [Russia] to act. And we've given [Russia] enough information to act on who that is'[342]

hereby suggesting that in principle any ransomware operation triggers due diligence duties to prevent harm. Yet, such an approach seems so far to be an outlier. Taking a quantitative approach, Art. 3 lit. d of the EU Council Cyber Sanctions Decision of May 2019 concerning 'restrictive measures against cyber-attacks threatening the Union or its Member States' determines the 'amount of economic loss' as a relevant factor for determining the question whether a cyber attack has a 'significant effect'.[343] More open-endedly, Art. 3 lit. a lists the 'disruption of economic activities' as a relevant criterion for the determination of malicious cyber activities with a 'significant effect'[344] and specifies the 'scope, scale, impact or severity'[345]

342 CNN, 'Biden warns Putin during call that 'we expect him to act' on Russian ransomware attacks', *CNN* 9 July 2021, available at: https://edition.cnn.com/2021/07/09/politics/biden-putin-call-syria-ransomware/index.html.

343 Council of the European Union, Decision 7299/19 2019 (n.330), art. 3: 'The factors determining whether a cyber-attack has a significant effect as referred to in Article 1(1) include (…) (d) the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property'.

344 Ibid., art. 3a. The classification of a significant effect 'only' triggers the applicability of restrictive measures – as retorsion – and hence is not tantamount to a categorization as internationally wrongful. It nevertheless indicates legal criteria based on which states will respond to a malicious operation.

345 Council of the European Union, Decision 7299/19 2019 (n. 330), art. 3a.

and the 'numbers of persons affected' as criteria for assessing whether a cyber operations has a significant effect.[346] Similarly open-endedly the Czech Republic considered a significant impact on its economy as a relevant factor for the question if an act amounts to a violation of international law.[347] The now-repealed EU Directive on the security of network and information system (NIS) 2016/1148 stipulated the market share of an entity and the geographical scope of its economic operations as criteria to determine when cyber operations have significant disruptive effects on the provision of critical services.[348] While these criteria concerned disruptive effects on critical infrastructure they seem equally useful for the general assessment of the significance of economic harm.

None of the above-mentioned criteria have been sufficiently endorsed by states to be considered *lex lata* and hence so far have only exemplary character. As a bottomline, however, the various examples of open-ended sliding-scale criteria weigh against assuming significant economic cyber harm already at a very low-level, e.g. with regard to a single ransomware operation. However, it should be recalled that also many minor harmful acts which on their own do not reach the significance threshold may cumulatively be considered significant harm, as the *Trail Smelter* case shows.[349]

4. Economic harm as an emerging category of significant cyber harm

Economic cyber harm is a strong candidate for significant harm under the harm prevention rule. Due to the manifold economic ramifications of cyber operations and insufficient opinio iuris it is however difficult to comprehensively assess which economic cyber harm is most relevant. It is clear that states are particularly concerned about theft of intellectual property and trade secrets via economic cyber espionage. However, it is so far unclear if *any* theft of intellectual property or trade secrets is considered

346 Ibid., art. 3b.

347 In the context of a potential sovereignty Czech Republic, 'Statement UN OEWG' 2020 (n. 195), p. 3.

348 Directive (EU) 2016/1148, 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union, art. 6 lit. d, e. The directive uses the term essential service but this is largely equivalent to critical infrastructure, see the similarity of the definition of essential service, art. 5 (2), to the understanding of critical infrastructure in the international legal discourse, below chapter 3.C.II.3.

349 See above chapter 3.A.V.

significant, hereby triggering due diligence obligations to prevent. States are well advised to specify their opinio iuris in this regard. The same applies to the more ambiguous question which degree of economic harm beyond access operations amounts to significant harm, e.g. under which circumstances ransomware operations amount to significant harm. A variety of potential quantitative and qualitative criteria exist, yet states have not yet sufficiently endorsed them.

II. Cyber harm to critical infrastructure as a category of significant cyber harm

A further category of significant cyber harm may be cyber harm to critical infrastructure. Malicious cyber operations against critical infrastructure are a grave threat for both national and international security. In December 2015 the attack with *Black energy* malware caused power outage for six hours to hundreds of thousands of homes in the Ukraine.[350] In the US, ransomware paralyzed a hydroelectric power plant.[351] Malicious cyber operations against hospitals during the COVID-pandemic with ransomware disabled the delivery of medical services during an acutely vulnerable period.[352] In May 2020, an Iranian port was targeted by malicious cyber operations for several days, its operation was disrupted, causing traffic jams and delays in shipment.[353] In September 2020, a cyber operation against a German hospital caused delayed treatment of a woman who had to be

350 Kim Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', *Wired,* 3 March 2016, available at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

351 Jan Kleijssen/Pierluigi Perri, 'Cybercrime, Evidence and Territoriality: Issues and Options', in Martin Kuijer/Wouter Werner (eds.), *The Changing Nature of Territoriality in International Law* (Netherlands Yearbook of International Law 2016), 147–173, at 153.

352 See the condemnation by Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic, 30 April 2020: 'Since the beginning of the pandemic, significant phishing and malware distribution campaigns, scanning activities and distributed denial-of-service (DDoS) attacks have been detected, some affecting critical infrastructures that are essential to managing this crisis (…) Any attempt to hamper the ability of critical infrastructures is unacceptable.'

353 Ronen Bergman/David M Halbfinger, 'Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks', *New York Times*, 18 May 2021, available at: https://www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyberattacks.html.

transferred to another hospital and subsequently died.[354] The list of cyber operations against critical infrastructure could be extended substantially, yet the list of attempted attacks is even longer. For example, in April 2020, hackers unsuccessfully tried to penetrate the SCADA of wind turbines in Azerbaijan; in another case, hackers unsuccessfully tried to penetrate the command and control system of water treatment plants, pumping stations and sewages in Israel.[355] There are further instances in which potentially devastating consequences of malicious cyber operations could be averted. It is hence evident that malicious cyber operations against critical infrastructure can have the gravest consequences for nation states, society and individuals.[356]

1. Increasing concern about cyber operations against critical infrastructure

The concern about cyber harm to critical infrastructure is a 'cross-cutting theme' in UN resolutions since the turn of the millennium.[357] The UN GGE Report of 2015 stated:

> 'The most harmful attacks using ICTs include those targeted against the critical infrastructure and associated information systems of a State. The risk of harmful ICT attacks against critical infrastructure is both real and serious.'[358]

354 Although it is not clear whether the death could have been avoided without the delayed treatment Melissa Eddy/Nicole Pelroth, 'Cyber Attack Suspected in German Woman's Death', *New York Times*, 18 September 2020, available at: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.

355 For a continuously updated list of international cyber incidents, including the two mentioned here see https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

356 Eric Talbot Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense' *Stanford Journal of International Law* 38 (2002), 207–240, at 207.

357 Michael Berk, 'Recommendations 13 (g) and (h)', in Eneken Tikk (ed.) *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary,* (United Nations Office for Disarmament Affairs 2017), 191–222, at 197, 198, paras. 14, 15.

358 UN GGE Report 2015, para. 5.

The UN OEWG Final Report highlighted the potentially 'devastating consequences' of malicious cyber operations against critical infrastructure.[359] Also the UN GGE Report 2021 noted the increasingly serious character of malicious cyber operations against critical infrastructure.[360] Therefore, it is clear that malicious cyber operations against critical infrastructure have become a core concern of states in international law.

2. Diverging definitions of critical infrastructure

The commentaries to the Budapest Convention provide a widely agreeable bottomline of what critical infrastructure is. According to this commentary critical infrastructure

> 'can be defined as systems and assets, whether physical or virtual, so vital to a country that their improper functioning, incapacity or destruction would have a debilitating impact on national security and defence, economic security, public health or safety, or any combination of those matters.'[361]

States' precise definitions of critical infrastructure however diverge. Some are extremely wide, like the one by Russia which would potentially include any governmental agency as critical infrastructure.[362] The definition of the

359 UN OEWG Final Report 2021, para. 18: 'States concluded that there are potentially devastating security, economic, social and humanitarian consequences of malicious ICT activities on critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public.'

360 UN GGE Report 2021, para. 10: 'Harmful ICT activity against critical infrastructure that provides services domestically, regionally or globally, which was discussed in earlier GGE reports, has become increasingly serious.'

361 Cybercrime Convention Committee (T-CY), T-CY Guidance Notes, T-CY (2013)29, 8 October 2013, p. 15; the Tallinn Manual gives a similar definition, Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), Glossary, p. 564: 'Physical or virtual systems and assets of a State that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment.'

362 Russia, Federal Law of the Russian Federation, 26 July 2017, No. 187-FZ, art. 2: 'Critical infrastructure facilities" shall mean facilities, systems and institutions of the state which conduct their activities in the interests of the state, national defense or security, including individual security'.

US also includes commercial facilities[363], while the definition of Uruguay includes 'any service that affects more than 30 % of the population'.[364]

Despite all deviations it is notable that almost all definitions list a number of key critical infrastructures: These are medical services, financial services, governmental services, food, transportation, communication, energy and water supply.[365]

Beyond these key critical infrastructures states deviate in their designation of sectors and entities as critical infrastructure. It is for example unclear whether electoral processes are considered critical infrastructure.[366] Considering that globally a significant number of states are not democratic and that furthermore also democratic states like the US have only added electoral infrastructure to the list of critical infrastructure in January 2017[367] this tentatively weighs against assessing electoral processes as critical infrastructure. Furthermore, interference with electoral processes may violate the prohibition of intervention.[368] Consequently, strengthening their protection by categorizing it as critical infrastructure does not seem necessary in order to grant them due protection under international law.

363 US, White House, 'Critical Infrastructure Security and Resilience' (2013) Presidential Policy Directive/PPD-21.

364 Uruguay, Comments on the pre-draft of the UN OEWG report, p. 3, para. 5.

365 Delerue, 'Cyber Operations' 2020 (n. 107), 298; ITU, Guide to Developing a National Cybersecurity Strategy, 2018, p. 42; see e.g. Australia Department of Home Affairs, Critical infrastructure resilience, names banking and finance, government, communications, energy, food and grocery, health, transport, water as critical infrastructure, available at: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/critical-infrastructure-resilience.

366 In favour e.g. Netherlands, 'International Law in Cyberspace' 2019 (n. 15), Netherlands; see also mention in Final Report, UN OEWG, para. 18.

367 US, DHS, Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, 6 January 2017, available at: https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical; a statement by Germany in the UN OEWG suggests that it considers electoral infrastructure critical infrastructure see Germany, Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security, Comments from Germany, 6 April 2020, para. 31: 'we consider the proposals to protect the public core of the internet, not to disrupt the infrastructure essential to political processes, not to harm medical facilities and to highlight transnational infrastructure as useful additions to the already existing norms on the protection of critical infrastructure as contained in the 2015 GGE report.'

368 On electoral processes as part of the domaine réservé see above chapter 3.B.II.2.3.1.

A further contentious question is whether high governmental institutions, such as ministries or other executive bodies, should be considered critical infrastructure. The US for example designates 'government facilities' as critical infrastructure.[369] Also China designates 'e-government' and 'public services' as critical infrastructure in its Cybersecurity Act of 2017, albeit in the context of an otherwise overly broad list of critical infrastructure.[370] Designating government facilities as critical infrastructure may be prima facie plausible as e.g. the hampering of high-level ministeries or of the head of a government may affect the political stability of a state. However, the notion of governmental facilities in the cited documents cannot be sufficiently narrowed down. This eventually weighs against including governmental facilities as a distinct category of critical infrastructure under international law.

In light of the divergent definitions states and commentators have argued for a common definition of critical infrastructure. In the UN OEWG, Egypt e.g. highlighted that such a common definition could be helpful to make the prohibition to damage or otherwise impair the use and operation of critical infrastructure more effective.[371] Also Pakistan has pushed for moving forward with a definition of critical infrastructure.[372] As defining critical infrastructure is considered a confidence-building measure (CBM) in the UN OEWG Zero Report[373] it seems likely that states will continue to specify their understanding of critical infrastructure. In doing so, they

369 US, DHS, 'Statement' 2017 (n. 367).

370 Daniel Albrecht, 'Chinese Cybersecurity Law Compared to EU-NIS-Directive and German IT-Security Act', *Computer Law Review International* 19 (2018), 1–5: '[Critical information infrastructure] includes traditionally sensitive sectors such as public telecommunications and information services, energy, transportation, irrigation, finance, public services, e-government, but also includes the catch-all phrase "as well as other areas that may harm national security, the economy, and the public interest"'.

371 Egypt, Comments on the Pre-Draft report, 2020, p. 3: 'Member States should be encouraged to reach an agreed common definition of what constitutes "critical infrastructure", with a view to agreeing, as appropriate, on prohibiting any act that knowingly or intentionally utilizes offensive ICT capabilities to damage or otherwise impair the use and operation of critical infrastructure.'

372 Pakistan, Pakistan's inputs in response to the letter dated 11 March 2020 from the Chair of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (UN OEWG), p.2, para. 11.

373 UN OEWG, Zero Draft Report 2021, para. 63.

may consider a hierarchy of critical infrastructure facilities.[374] However, eventually designation of critical infrastructure is a national prerogative, as acknowledged by the UN GGE Report 2021[375] and by several states in the UN OEWG.[376] To expect a homogenous definition of critical infrastructure in the near future seems hence futile.

III. Increasing concern about harm to the public core of the internet

States have shown an increasing concern over harmful cyber operations that affect the integrity and availability of the internet.[377] In 2011 a CoE Advisory Report underlined the need to protect the internet.[378] In the Paris Call of 2018 states vowed to prevent activities that damage the general

374 Melissa Hathaway, 'Introduction: International Engagement on Cyber V: Securing Critical Infrastructure', *Georgetown Journal of International Affairs* (2015), 3–7.

375 UN GGE Report 2021, para. 44: '(…) each State determines which infrastructures or sectors it deems critical within its jurisdiction, in accordance with national priorities and methods of categorization of critical infrastructure.' para. 45: 'Highlighting these infrastructures as examples by no means precludes States from designating other infrastructures as critical, nor does it condone malicious activity against categories of infrastructures that are not specified above.'

376 Canada, Proposed norms guidance text, UN OEWG, 11 February 2021, p. 5: 'Each State determines which infrastructures or sectors it deems critical, in accordance with national priorities and methods of categorization of critical infrastructure'; Statement by South Africa at the Informal UN OEWG, 22 February 2021, p.1: '(…) the designation of national critical infrastructure and national critical information is a national competence'.

377 Dennis Broeders, *The Public Core of the Internet* (Amsterdam: Amsterdam University Press 2015), p. 11: 'The need for worldwide consensus on the importance of a properly functioning public core of the Internet seems obvious because it is these protocols that guarantee the reliability of the global Internet.'

378 The CoE Avisory Report explicitly calls for a context-specific assessment of impacts on the 'security, stability,robustness and resilience' of the internet, CoE, Steering Committee on the Media and New Communication Services (CDMC), Explanatory Memorandum to the draft Recommendation CM/Rec(2011) of the Committee of Ministers to member states on the protection and promotion of Internet's universality, integrity and openness, CM(2011)115-add1 24 August 2011, para. 51. Global Commission on the Stability of Cyberspace (GCSC), Call to Protect the Public Core of the Internet (New Delhi, November 2017), https://cyberstability.org/wp-content/uploads/2018/07/ call-to-protect-the-public-core-of-the-internet.pdf. An early proponent of identifying the public core of the Internet for special protection was Dennis Broeders, a Dutch researcher.

availability and integrity of the public core of the internet.[379] In 2019, the GCSC proposed a norm against the intentional and substantial damaging of the general availability and integrity of the public core[380], endorsed by the Organization for Security and Co-operation in Europe (OSCE) in 2019.[381] Also the UN OEWG Report and several states in the UN OEWG underlined the need to protect the integrity of cyberspace.[382] The increasing concern about harm to the public core of the internet is further evidenced by its repeated assertion as critical infrastructure.[383] The UN GGE Report 2021 for example asserted the technical infrastructure essential to the general availability and integrity of the internet as critical infrastructure.[384] This seems to suggest that harm to the public core of the internet may be conceived as a sub-category of harm to critical infrastructure. However, as harm to the public core of the internet may affect the international community as a whole – in contrast to harm to critical infrastructure

379 Paris Call (n. 11) 2018, p.3: 'To that end, we affirm our willingness to work together, in the existing fora and through the relevant organizations, institutions, mechanisms and processes to assist one another and implement cooperative measures, notably in order to: (…) Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet'.

380 GCSC, Final Report 2019, Proposed Norms, p. 21, Norm 3: 'State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace.'

381 Reiterated in OSCE, Bratislaca, Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 2019, p.20.

382 UN OEWG, Final report, para. 26: 'While agreeing on the need to protect all critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public, along with endeavouring to ensure the general availability and integrity of the Internet, States further concluded that the COVID19 pandemic has accentuated the importance of protecting healthcare infrastructure including medical services and facilities through the implementation of norms addressing critical infrastructure. such as those affirmed by consensus through UN General Assembly resolution 70/237.'

383 Germany, 'Comments' 2020 (n. 367), para. 31.

384 UN GGE Report 2021, para. 45: '(…) Critical infrastructure may also refer to those infrastructures that provide services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet. Such infrastructure can be critical to international trade, financial markets, global transport, communications, health or humanitarian action.'

which primarily affects the interests of the respective territorial state – it is preferable to distinguish the former from the latter.[385]

Regardless of this categorical question, all above-mentioned positions show a growing concern over cyber harm to the public core of the internet. This suggests that it may be considered an emerging category of significant harm under the harm prevention rule. In this vein, the CoE Report of 2011 linked the protection of the global internet to due diligence and asserted that harm to the internet may be considered significant harm.[386]

Regarding the precise protective scope of such an emerging category states, experts and commentators have either referred to the need to protect the 'general availability or integrity'[387], the public core of the internet[388], or a combination of both.[389] According to the GCSC the public core includes the 'packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, transmission media, software, and data centers'.[390] In the EU Cybersecurity Act at least 'the key protocols, the domain name system and the root zone'[391] were defined as

385 On the interest of the international community in the proper functioning of the internet see Netherlands, The Kingdom of the Netherlands' response to the pre-draft report of the UN OEWG, 2020, paras. 28, 29: '(…) adequate protection of (…) critical infrastructures would benefit the international community (…) Of this development, the internet itself is the best example (…).' On the international community as a rightholder in cyberspace, as well as on the possibility to take collective countermeasures, see chapter 5.C.IV.

386 CoE, 'Advisory Report' 2011 (n. 378), para. 78: 'This principle states that, within the limits of non-involvement in the day-to-day technical and operational matters, states should, in co-operation with each other and with all relevant stakeholders, take all necessary measures to prevent, manage and respond to significant transboundary disruptions to, and interferences with, the infrastructure of the Internet, or at any event minimise the risk and consequences arising from such events.'

387 GCSC, 'Final Report' 2019 (n. 380), norm 3.

388 The EU Cybersecurity Act, Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act), Rc. 23.

389 For an equivalent understanding of the public core and the general availability and integrity of the internet see Przemysław Roguski, 'Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea?' in Taťána Jančárková/Lauri Lindström et al. (eds.), *20/20 Vision: The Next Decade* (NATO CCDCOE 2020), 25–42, at 38, 39.

390 GCSC, 'Final Report' 2019 (n. 380), p. 31.

391 Roguski, 'Collective Countermeasures' (n. 389), 37: 'There is growing consensus that the public core of the internet should at least include the key protocols, the domain name system and the root zone, as described in the EU Cybersecurity Act.'

the public core, partially concurring with a Dutch expert report from 2016 which also determined the main protocols of the internet as the public core.[392] Hence, so far, slight divergences regarding the precise definition of harm to the public core exist. In light of the growing attention to this subject it seems plausible that states may specify their understanding of the public core in the future.

IV. Cyber espionage as a category of significant cyber harm

Cyber espionage operations are pervasive in international relations and have become a cross-cutting threat dimension across various areas. The increasing concern over the harmful effects of various forms of cyber espionage can inter alia be seen in the discussion concerning a potential prohibitive sovereignty rule in cyberspace in which proponents of the pure sovereigntist approach have underlined the harmfulness of cyber espionage[393] and in which at least one country explicitly considered espionage operations a potential violation of a prohibitive sovereignty rule.[394] In the context of the harm prevention rule the increasing concern over cyber espionage raises the question if and under which circumstances cyber espionage operations may be considered significant harm, hereby entailing a negative duty on states not to conduct such operations, as well as due diligence duties to prevent such operations by non-state actors under their jurisdiction or control.

392 Mostly focussing on the 'main protocols of the internet' Broeders, 'Public Core' 2015 (n. 377), 105: 'These new coalitions should work towards the establishment of an international norm that identifies the main protocols of the Internet as a neutral zone in which governments are prohibited from interfering for their own national interests'; 47: 'They come up with ideas for protocols and standards that regulate data transfer, interoperability, interconnection and routing between networks, and the format of the data transmitted across the Internet'.

393 Heller, 'Pure Sovereignty' 2021 (n. 190), 1499.

394 Costa Rica, 'Costa Rica's Position' 2023 (n. 243), para. 22; see above chapter 3.B.III.5.i.

1. The legality of espionage in international law

Espionage in general and cyber espionage in particular has an ambivalent role in international law.[395] On the one hand, espionage is asserted as a valuable tool for collective security[396] and for a better understanding of a state's negotiating position.[397] On the other hand, states frequently protest against espionage operations which target them and prosecute spies, while not formally objecting to each and every espionage operation.[398] Tolerance of espionage operations has been likened to the acceptance of a 'necessary evil'.[399]

The legality of espionage in international law lies in a legally grey area. Some commentators argue that extensive states practice shows that states have a right to spy[400], or that it is at least not illegal under international law as no prohibitive rule exists.[401] Other commentators argue that espionage is illegal under international law, contending that espionage violates the prohibition of intervention and territorial sovereignty.[402] Again other commentators have argued that espionage is neither legal nor illegal under international law.[403] The legality of espionage is hence at best ambiguous. In cyberspace, this result is unsatisfactory: Due to the enhanced access to devices, computer systems and content thereon, espionage operations

395 Simon Chesterman, 'Secret Intelligence', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2009), para. 3.

396 Ibid., para. 29.

397 Christopher D. Baker, 'Tolerance of International Espionage: A Functional Approach', *American University International Law Review* 19 (2003), 1091–1113, at 1104.

398 Moynihan, 'The Application of International Law' 2019 (n. 58), para. 144.

399 Chesterman, 'Secret Intelligence' (n. 395), para. 23.

400 Asaf Lubin, 'The Liberty to Spy', *Harvard International Law Journal* 61 (2020), 185–243; Gary Brown/Keira Poellet, 'The Customary International Law of Cyberspace', *Strategic Studies Quarterly* 6 (2012), 126–145, at 133–134.

401 Stefan Talmon, 'Das Abhören des Kanzlerhandys und das Völkerrecht', *Bonn Research Papers on Public International* Law 3 (2013), at 6.

402 Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs', in Roland J. Stanger (ed.), *Essays on Espionage and International Law* (Columbus: Ohio State University Press 1962), 3 at 5, 12–13; Ian H. Mack, *Towards Intelligent Self-Defence: Bringing Peacetime Espionage in From the Cold and Under the Rubric of the Right of Self-Defence* (Sydney Law School 2013), at 4, 21–22.

403 Helmut Philipp Aust, 1. Untersuchungsausschuss der 18. Wahlperiode des Deutschen Bundestages Stellungnahme zur Sachverständigenanhörung am 5. Juni 2014, p. 14, para. 37, Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 32, p. 170.

have reached unprecedented levels in scale and scope.[404] This has made the question of the legality of cyber espionage ever more pressing.

Increasingly, commentators argue that international law prohibits cyber espionage per se[405], or at least some forms of cyber espionage operations.[406] A blanket ban of cyber espionage operations seems unrealistic but there is increasing evidence that the concern about cyber espionage has attained a cross-cutting dimension. Apart from the increasing concern about economic cyber espionage[407] this is particularly obvious with regard to bulk surveillance practices, as well as with regard to espionage operations which target governmental and international institutions.

2. Increasing concern about harm caused by mass surveillance operations

In 2013, the 'Snowden leaks' revealed the mass surveillance practices of the US intelligence service NSA. Inter alia under a programme code-named PRISM the NSA conducted foreign surveillance via spyware on individuals to collect personal data. Globally, meta and content data of individuals, as well as their communications, were intercepted and collected on an indiscriminate basis[408], inter alia through secret surveillance backdoors installed by technology companies[409], as well as through the sharing of surveillance

404 Mueller, 'Against Sovereignty' 2020 (n. 251), 788.

405 Heller, 'Pure Sovereignty' 2021 (n. 190), 1499; Buchan, 'Eye on the Spy' 2021 (n. 250): 'By penetrating computer networks and systems in order to steal confidential data, cyber espionage operations can interfere with privacy-related rights, undermine trust and confidence in digital infrastructure, disrupt the delivery of essential services and, in extreme cases, threaten national security. International law must therefore prohibit cyber espionage and deter this activity.'

406 Arguing that espionage is illegal under international law if it causes harmful effects Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 32, p. 170, para. 6; arguing that espionage is illegal under international law if it amonts to the exercise of state power, with further explanations Roguski, 'Territorial Sovereignty' 2020 (n. 133), 79.

407 See above chapter 3.C.I on economic cyber harm as a distinct category of significant harm under the harm prevention rule.

408 James Risen/Eric Lichtblau, 'How the U.S. Uses Technology to Mine More Data More Quickly', *New York Times,* 8 June 2013, available at: https://www.nytimes.com/2013/06/09/us/revelations-give-look-at-spy-agencys-wider-reach.html.

409 Talita de Souza Dias/Antonio Coco, *Cyber due diligence in international law* (Print version: Oxford Institute for Ethics, Law and Armed Conflict 2021), 79.

data of intelligence services of other countries.[410] After the revelations several states protested strongly against the mass surveillance programme and denounced its harmful impact on human rights. Resolution 68/167 of the UN General Assembly for example highlighted the detrimental impact of surveillance on the exercise and enjoyment of human rights.[411] Also the then-Brazilian president Rouseff repeatedly emphasized the harmful impact of mass surveillance on human rights.[412]

In the context of the harm prevention rule the concern about mass surveillance raises the question whether mass surveillance operations which are conducted extraterritorially, e.g. through the interception of extraterritorial data flows, can be considered significant harm. As such surveillance operations affect human rights the compatibility of such operations with human rights law comes into focus.

Before turning to this analysis it is important to note that the legality (or illegality) under human rights law is in principle without prejudice to its legal assessment as significant harm under the harm prevention rule. Hence, even if extraterritorial cyber espionage violates human rights law this does not necessarily imply that this human rights violation amounts to significant harm under the harm prevention rule. Conversely, even if extraterritorial cyber espionage is compatible with human rights law this does not preclude that it may be considered significant harm under the harm prevention rule.[413] Yet, the question whether mass surveillance violates human rights law is nevertheless relevant for the question whether it constitutes significant harm under the harm prevention rule. Art. 2 lit. b of the ILC Draft Articles on Prevention shows that harm to persons and

410 Edward Snowden: Germany a 'primary example' of NSA surveillance cooperation, *DWNews* 17 September 2019, available at: https://www.dw.com/en/edward-snowden-germany-a-primary-example-of-nsa-surveillance-cooperation/a-50452863.

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

412 Statement by H.E. Dilma Rousseff at the Opening of the General Debate of the 68th Session of the UN General Assembly, 24 September 2013: 'We face (…) a situation of grave violation of human rights and of civil liberties; of invasion and capture of confidential information concerning corporate activities (…)'.

413 Such a finding could for example be based on the harmful impact of bulk surveillance programmes on the broader societal level, e.g. for consumer trust in the confidentiality of ICT products.

property infuences whether harm is significant under the harm prevention rule.[414] Furthermore, already the *Arjona* case before the US Supreme Court showed the potential link between the harm prevention rule and human rights law: The Court implicitly held that a harmful impact on the rights of individuals on the territory of another state may implicate the harm prevention rule.[415] Compliance with human rights law is hence informative for the assessment of significant harm under the harm prevention rule, but does not prejudice it.

Under international human rights law, a central issue regarding the legality of bulk surveillance is the extraterritorial scope of human rights obligations. A key question in this regard is whether extraterritorial espionage[416] is within the jurisdictional scope of human rights law.[417] Commentators had supported this argument for a long time[418] but particularly the US had advocated for a restrictive interpretation.[419] In recent years several courts have acknowledged the extraterritorial application of human rights or have at least not opposed it. The German Federal Constitutional Court for example acknowledged that the guarantee of the privacy of telecommunications also applies to extraterritorial surveillance operations.[420] The decision concerned constitutional rights under the German constitution but the Court explicitly noted the human rights law dimension of the

414 Acknowledging the relevance of human rights impacts under the harm prevention, see also ILC Draft Articles on Prevention (n. 6), art. 2b: ' "Harm" means harm caused to persons, property or the environment'.

415 US Supreme Court, *United States v. Arjona*, 7 March 1887, 120 U.S. Reports 1887, 484: 'The law of nations requires every national government to use "due diligence" to prevent a wrong being done within its own dominion to another nation with which it is at peace, or *to the people* thereof' (emphasis added).

416 I.e. intelligence practices that intercept data flows on foreign territory, e.g. via satellite.

417 For an overview of problematic jurisdictional implications of mass surveillance see Milan Tahraoui, 'Surveillance des flux de données: juridiction ou compétences de l'État, des notions à refonder', in Matthias Audit/Etienne Pataut (eds.), *L'extraterritorialité* (Paris: Pedone 2020), 141–194, at 170f.

418 Beth van Schaack, 'The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change', *International Law Studies* 90 (2014), 20–65; Helmut Philipp Aust, 'Spionage im Zeitalter von Big Data – Globale Überwachung und der Schutz der Privatsphäre im Völkerrecht', *Archiv des Völkerrechts* 52 (2014), 375–406, at 394f.

419 UN Human Rights Committee, Concluding Observations on the Fourth Report of the United States of America, adopted by the Committee at its 110th session, 10–28 March 2014, advance unedited version, para. 4.

420 BVerfG, Judgment of the First Senate of 19 May 2020, 1 BvR 2835/17, paras. 97, 98.

case.[421] In a subsequent decision the European Court of Human Rights (ECtHR) Grand Chamber avoided the question in *BigBrotherWatch* and simply assumed that extraterritorial surveillance is within a country's jurisdiction as the defendant in the case, the UK, had not raised a jurisdictional objection.[422] In *Wieder and Guarnieri v. UK* the ECtHR again avoided general remarks on the extraterritorial applicability of the ECHR. Yet, it held that interference with the data of an individual implicates the right to privacy under the convention, even if the individual is not located on the territory of the interfering state, hereby giving the judgment an undeniable relevance for the question whether the ECHR applies extraterritorially.[423] Also the Tallinn Manual assumed that cyber espionage operations could violate human rights, without however specifying under which circumstances this would be the case.[424] There are hence indicators of increasing acknowledgment of the extraterritorial applicability of international human rights law regarding privacy interferences in cyberspace, parallel to the recognition of the extraterritorial applicability of human rights law in other areas of international law, based on 'effective'[425] or 'functional' authority and control.[426]

421 Ibid.

422 ECtHR, *Case of Big Brother Watch and Others v the United Kingdom*, Grand Chamber Judgment of 25 May 2021, Applications Nos. 58170/13, 62322/14 and 24960/15, para. 272; critical in this regard Marko Milanovic, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa', *EJIL:Talk!,* 26 May 2021 available at: https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/.

423 ECtHR, *Case of Wieder and Guarnieri v. the United Kingdom*, Judgment of 12 September 2023, Applications nos. 64371/16 and 64407/16), paras. 94, 95; on the extraterritorial dimension of the case see Marko Milanovic, 'Wieder and Guarnieri v UK: A Justifiably Expansive Approach to the Extraterritorial Application of the Right to Privacy in Surveillance Cases', *EJIL:Talk!,* 21 March 2024, available at: https://www.ejiltalk.org/wieder-and-guarnieri-v-uk-a-justifiably-expansive-approach-to-the-extraterritorial-application-of-the-right-to-privacy-in-surveillance-cases/.

424 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 1), commentary to rule 32, p. 170, para. 6: '[I]f cyber operations that are undertaken for espionage purposes violate the international human right to privacy (…) the cyber espionage operation is unlawful.'

425 ECtHR, *Loizidou v. Turkey (preliminary objections)*, Judgment of 23 March 1995, Application No. 15318/89, para. 88; UK Court of Appeal in the R., (*Al-Skeini) v. Secretary of State for Defence*, [2005] EWCA Civ. 1609.

426 Yuval Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law', *The Law & Ethics of Human Rights* 7 (2013), 47–71; Buchan, 'Cyber Espionage' 2018 (n. 190), 105.

On the substantive level, however, courts have so far shown leniency with regard to the outer limits of cyber espionage and have been largely deferential to states' practices. In *Big Brother Watch*, the ECtHR Grand Chamber for example rejected the argument that mass surveillance measures (on content and meta data, as well as communications) are disproportionate per se.[427] It only required that states put procedural safeguards in place, such as time limits and procedures for authorizing the selection of intercepted material, and supervision by an independent authority.[428] The ECtHR notably even stated that the collection of data did not constitute 'a particularly significant interference with privacy'.[429] This leniency tentatively weighs against the argument that bulk surveillance operations constitute significant harm under the harm prevention rule.

Aside from human rights interferences, the argument for the significance of harm caused by mass surveillance operations may however also be based on their harmful impact on the mutual trust between states. The European Commissioner for Home Affairs Malmström highlighted that the revealed mass surveillance operations harmed mutual trust and confidence between states[430] and that this may potentially affect inter-state cooperation on terrorist or criminal threats.[431] Commentators have also highlighted the broader societal harmful impacts of mass surveillance, for example on the

427 Suggesting that mass surveillance is neither necessary nor proportionate UN General Assembly Resolution A/RES/68/167, 'Right to privacy in the digital age', 18 December 2013, para. 26.

428 ECtHR, 'Big Brother Watch' (n. 422), para. 350: 'In order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "end–to–end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review.'; The judgment was criticized for its insufficient proportionality assessment see Milanovic, 'The Grand Normalization' 2021 (n. 422).

429 ECtHR, 'Big Brother Watch' (n. 422), para. 330.

430 Adrian Croft, 'EU Threatens to Suspend Data-sharing with U.S. over Spying Reports', *Reuters,* 5 July 2013, available at: https://www.reuters.com/article/usa-security-eu-idINDEE96409F20130705; on damage to mutual see also Michael Knigge, 'NSA surveillance eroded transatlantic trust', *DW*, 27 December 2013, available at: https://www.dw.com/en/nsa-surveillance-eroded-transatlantic-trust/a-17311216.

431 'EU says distrust of US on spying may harm terror fight', *BBC*, 25 October 2013, available at: https://www.bbc.com/news/world-europe-24668286.

rule of law and democractic participation, or institutional trust.[432] However, as states continue to pursue extraterritorial bulk surveillance measures, more opinio iuris would be necessary to conclude that a sufficient amount of states indeed consider such harmful impacts significant harm under the harm prevention rule. As a matter of *lex lata,* hence, cyber harm caused by mass surveillance operations cannot be considered an emerging category of significant harm under the harm prevention rule.

3. Increasing concern about cyber espionage operations against governmental and international institutions

States have furthermore increasingly expressed concern about cyber espionage operations against governmental and international institutions. In July and October 2020 the EU took restrictive measures against several individuals and the Russian intelligence service GRU which was accused of having hacked the German parliament in 2015.[433] In doing so, it based its decision on the grounds that the parliament's 'ability to operate' was 'affected', thereby causing a 'significant effect' which constituted an external threat in the meaning of Art. 1 (1) of Council Decision 7299/19.[434] It also referred to amounts of data stolen' and the compromising of email addresses.[435] While the measure was a retorsive measure and therefore not based on an alleged violation of international law it indicates that the outer limits of acceptable state behaviour had been reached in this case. As a further example of concerns about cyber espionage operations against public institutions in October 2018, the Netherlands and the UK called out Russia for an attempted hack of the Organization for the Prohibition of Chemical Weapons (OPCW) in The Hague. During the operation the Wi-fi networks were targeted through the exploitation of hardware vulnerabilities

432 Neil M. Richards, 'The Dangers of Surveillance', *Harvard Law Review* 126 (2013) 1934–1965, at 1963; Andreas Lichter/Max Löffler/Sebastian Siegloch, 'The Long-Term Costs of Government Surveillance', *Journal of the European Economic Association* 19 (2021), 741–789, at 742.

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

434 Council of the European Union, Decision 2020/1537 (n. 159), Annex, para. 3.

435 Ibid.

at the building (i.e. a so-called close access operation).[436] The operation failed but the Netherlands, the territorial state hosting the OPCW, as well as the UK, which provided intelligence for detecting the attempt, released a statement that the operation demonstrated

> 'disregard for the global values and rules that keep us safe (…) We will uphold the rules-based international system, and defend international institutions from those that seek to do them harm'.

Additionally, cyber operations against heads of states have been condemned as violations of international law. The revelation that the phones of several heads of states, including the heads of states of Brazil, Mexico and Germany, were intercepted by the NSA for example prompted an international outcry.[437] Mexico e.g. condemned the spying of its president as 'unacceptable' and 'contrary to international law'. The concern over cyber operations against public institutions was also expressed in the UN OEWG Final Report of March 2021 which noted that:

> 'Malicious ICT activities against [critical infrastructure] and [critical information infrastructure] that undermine trust and confidence in political and electoral processes, public institutions (…) are also a real and growing concern'.[438]

It is notable that states not only protested against cyber espionage operations but also that they did so in the language of international law. In the context of the harm prevention rule it is furthermore noteworthy that when Belgium accused China of cyber espionage against its Ministry of the Interior and Defense in July 2022 it linked its concern about cyber espionage to due diligence obligations under the harm prevention rule. In what can be read as an implicit reference to the harm prevention rule it

436 'How the Dutch foiled Russian "cyber-attack" on OPCW', *BBC,* 4 October 2018, available at: https://www.bbc.com/news/world-europe-45747472.

437 UN General Assembly Resolution A/RES/68/167, 'Mexico Slams US Spying on President', *Der Spiegel,* 21 October 2013, available at: https://www.spiegel.de/international/world/mexico-condemns-reported-us-spying-by-nsa-on-president-calderon-a-929086.html quoting the Mexican foreign minister: 'This practice is unacceptable, illegitimate and contrary to Mexican law and international law'.

438 UN OEWG Final Report 2021, para. 18.

urged China to 'adhere to responsible state behavior norms (…) and to take action against such malicious activity originating from its territory'.[439]

Yet, there are also exceptions to this trend. The *SolarWinds* hack which became publicly known in December 2020 caused an international uproar.[440] Although inter alia the US Ministry of Defence was compromised the US fell short of calling out the *SolarWinds* infiltration a violation of international law. While the US imposed sanctions via an executive order[441] US president Biden merely called the operation 'inappropriate' and vowed that the US would respond in kind.[442] Beyond the *SolarWinds* example, it is also notable that the statements which invoke international law, such as the Dutch statement on the OPCW hack attempt, rarely specify legal criteria. Consequently, the legal contours of a putative legal limit of cyber espionage operations against governmental and international institutions remain unclear. The examples overall hence suggest an increasing concern about cyber espionage operations against governmental and international institutions but ambiguity as to which criteria are decisive for defining the outer limits of tolerated cyber espionage. Relevant criteria may e.g. be the importance of a public actor, interference with the operation of concerned institutions[443], significant replacement costs[444], the cumulative erosion of

439 Declaration by the Minister for Foreign Affairs on behalf of the Belgian Government urging Chinese authorities to take action against malicious cyber activities undertaken by Chinese actors, 18 July 2022, available at: https://diplomatie.belgium.be/en/news/declaration-minister-foreign-affairs-malicious-cyber-activities.

440 Patrick Beuth, 'Der Spionagefall des Jahres', *Der Spiegel,* 18 December 2020, available at: https://www.spiegel.de/netzwelt/netzpolitik/solarwinds-hack-der-spionagefall-des-jahres-a-0b728cc4-d375-4cb9-9450-3635ca8172a0.

441 US White House, 'Imposing Costs for Harmful Foreign Activities by the Russian Government', Press Release on Executive Order of 15 April 2021.

442 Ibid. Commentators have noted that the US likely conducts similar espionage operations against other countries which partially explain the reluctant reaction to the *SolarWinds* hack Jack Goldsmith, 'Self-Delusion on the Russia Hack', 18 December 2020, *The Dispatch*, available at: https://thedispatch.com/p/self-delusion-on-the-russia-hack?utm_campaign=post&utm_medium=web&utm_source=twitter.

443 Council of the European Union, Decision (CFSP) 2020/1125 of 30 July 2020, implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, Annex: 'The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work'.

444 Michael N Schmitt, 'Top Expert Backgrounder: Russia's SolarWinds Operation and International Law', *JustSecurity,* 21 December 2020, available at: https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.

public trust in such institutions[445], or the undermining of public trust in the integrity of IT.[446] As a consequence, cyber espionage operations against governmental and international institutions is thus an only cautiously emerging category of significant cyber harm.

Instead of grasping cyber espionage operations under the harm prevention rule – as e.g. Belgium has done – states may also move towards illegalizing certain forms of cyber espionage against governmental and international in the future via specific prohibitions.[447] In what could arguably be interpreted as a list of specific prohibitions of state-sponsored cyber espionage operations US President Biden sent the Russian president Putin a list of critical infrastructure targets that were 'off-limits' for attacks.[448]

V. Emerging legal yardsticks for risks of significant cyber harm

The preceding analysis has shown that several legal yardsticks for assessing whether a cyber operation amounts to a risk of significant harm can be discerned. It is clear that risks of cyber harm which – if they materialize – reach the threshold of a prohibitive rule, such as the prohibition on the use of force, the prohibition of intervention or a potential sovereignty rule, amount to risks of significant harm. Yet, it is regularly challenging to determine when the threshold of such prohibitive rules is reached. Further emerging categories of significant harm are economic cyber harm and cyber harm to critical infrastructure, as well as harm to the public core of the internet. Cyber espionage operations, such as bulk surveillance operations, or operations against governmental and international institutions, are of increasing concern in inter-state relations but the precise contours

445 On the relevance of this criterion in the context of non-intervention Germany, 'Application of International Law' 2021 (n. 68), p. 6.

446 E.g. concern regarding supply chain attacks, such as *Solar Winds*; see e.g.Written Testimony of Brad Smith President, Microsoft Corporation Senate Select Committee on Intelligence Open Hearing on the SolarWinds Hack, 'Strengthening the Nation's Cybersecurity: Lessons and Steps Forward Following the Attack on SolarWinds', 23 February 2021, p. 14: '(…) supply chain attacks that put technology users at risk and undermine trust in the very processes designed to protect them are out of bounds for state actors.'

447 Considering an illegalization of certain forms of cyber espionage in the future as a possible scenario Delerue, 'Cyber Operations' 2020 (n. 107), 200.

448 Vladimir Soldatkin/Humeyra Pamuk, 'Biden tells Putin certain cyberattacks should be 'off-limits'', *Reuters,* 17 June 2021, available at: https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16/.

of when such espionage operations amount to a risk of significant harm remain to be specified.