Chapter 4: Negative and Positive Obligations under the Harm Prevention Rule

The harm prevention rule entails two obligatory dimensions: The negative prohibitive dimension obliges states not to cause significant cyber harm.[1] The positive due diligence dimension obliges states to prevent and mitigate significant harm by non-state actors.[2]

A. The negative prohibitive dimension of the harm prevention rule

It is straightforward what states need to do to comply with the negative prohibitive dimension: They need to refrain from conducting cyber operations that cause significant harm. States for example need to refrain from cyber operations that likely cause significant economic harm or that amount to an internationally wrongful act.[3] States have highlighted the negative prohibitive dimension with regard to some categories of significant cyber harm.

I. Restrictive formulation regarding attacks on critical infrastructure in the UN GGE Reports

Regarding cyber operations against critical infrastructure the negative prohibitive dimension has received some nuance. States have underlined that critical infrastructure requires special protection under international law and should not be attacked. The UN GGE Reports stipulate a negative obligation[4] not to harm critical infrastructure

1 See chapter 2.A.VI.
2 See chapter 2.A.V.
3 On these categories of significant cyber harm see chapter 3.B and chapter 3.C.
4 The UN GGE Report introduces this obligation as a 'norm of responsible state behaviour'. On the regrettable ambiguity of this terminology in the UN GGE Reports and the preferable acknowledgment of such 'norms' as binding obligations see chapter 2.F.II.1.

> 'A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public'.[5]

The Final Report of the UN OEWG[6], the UN GGE Report 2021[7], as well as e.g. China[8] and the NAM have furthermore reiterated this negative obligation.[9] Egypt has called for a binding acknowledgement of the illegality of attacks against critical infrastructure in the UN OEWG[10] and also the African Group in the UN OEWG called for an explicit acknowledgement that cyber operations against critical infrastructure violate international law.[11] Albania and the US highlighted the norm to '[refrain] from damaging

5 United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), A/70/174, 22 July 2015 (UN GGE Report 2015), para. 13 lit.f.

6 UN OEWG Final Report 2021, para. 31.

7 United Nations, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UN GGE), A/76/135, 14 July 2021 (UN GGE Report 2021), paras. 42–46; See also UN General Assembly Resolution A/RES/73/27, 11 December 2018, para. 1.6.: 'A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.'

8 Statement by Minister-Counsellor Mr. Yao Shaojun at Arria Formula Meeting on Cyber Attacks Against Critical Infrastructure, 26 August 2020: 'The report of 2015 United Nations Group of Governmental Experts says clearly that a state should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure. However, some states still give authorization to conduct cyber attacks against critical infrastructure of other states. The practice is dangerous and does not serve the interests of all parties.'

9 UN OEWG Chairs Summary, 10 March 2021, A/AC.290/2021/CRP.3, p. 19: 'NAM stresses that all States should not knowingly conduct or support ICT activity in contrary to their obligations under international law that intentionally damages or impairs the use and operation of critical infrastructures.'

10 Remarks by Egypt at the Informal Meetings on the Zero Draft of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International security, p.1, para. 6: 'We continue to believe that there is a need for legally-binding obligations that would prohibit the use of ICTs against critical infrastructure facilities providing services to the public or for any purpose that is not consistent with International Law.'

11 Statement on Behalf of the African Group by H.E. Leon Kacou Adom, February 2021, p. 3, para. 6: '[W]e suggest to add an explicit reference that the use of ICTs to disrupt, damage, or destroy Critical Infrastructure and Critical Information Infrastructure represents a violation of International Law and the Charter obligations.'

critical infrastructure that provides services to the public'.[12] The duty not to impair critical infrastructure of other states is hence widely recognized.

The formulation of the negative obligation not to harm in the UN GGE Report is however restrictive in several aspects. First, it suggests that the negative prohibition only applies to *intentional* harm to critical infrastructure and not to accidental harm. The negative prohibitive dimension of the harm prevention rule however does not require intent in order to lead to accountability.[13] Also the Tallinn Manual acknowledged implicitly that already the causation of harmful effects may lead to the international wrongfulness of a cyber operation, regardless of intent.[14]

Second, the assertion that states should not 'conduct or knowingly support activities *contrary to [international law]* [emphasis added] that intentionally damages (…)' also suggests that intentional damage to critical infrastructure or its impairment is not *per se* contrary to international law. Such an interpretation would undermine the normative force of the rule. Statements of states indicate that the normative aim of para. 13 lit.f is precisely to prohibit attacks on critical infrastructure regardless of whether such acts violate further *distinct* rules of international law. The current formulation leaves such an interpretation however at least as a possibility.

Third, the reference to 'damage (…) or otherwise impairs the use and operation' likely excludes mere access operations (i.e. espionage operations). Access operations do not alter or delete data and hence cannot be said to cause damage or 'impair the use'. Hence espionage operations against

12 The statements followed a cyber operation which inter alia disrupted services of the Albania state police. Letter dated 7 September 2022 from the Permanent Representative of Albania to the United Nations addressed to the Secretary-General and the President of the Security Council, A/76/943-S/2022/677; US White House, Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania, 7 September 2022, available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/07/statement-by-nsc-spokesperson-adrienne-watson-on-irans-cyberattack-against-albania/.

13 Jelena Bäumler, *Das Schädigungsverbot im Völkerrecht* (Berlin: Springer 2017), p. 21; Jason D. Jolley, 'Recommendation para. 13f', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 169–190, at 188, para. 52.

14 In the context of an unintentionally harmful cyber espionage operation as a violation of sovereignty see Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press 2017), commentary to rule 32, p. 170, para. 6.

governmental institutions[15], such as in the *SolarWinds* hack, would not be covered by the negative prohibition. States are however increasingly concerned about such operations. The seemingly permissive formulation in para. 13 lit. f corresponds to the ambiguity as to the outer boundaries of espionage operations against such institutions (which in many cases can be considered critical infrastructure).[16] Only via an interpretation that would also include necessary IT replacement as disruptive cyber espionage operations against critical infrastructure would be covered under the rule. However, states have so far not adopted such an interpretation.

Therefore, while the reiteration of the negative obligation in para. 13 lit. f strengthens the normative force of the negative obligation and cements the relevance of harm to critical infrastructure as significant harm, its restrictive formulation risks to water down its protective purpose.

The UN GGE Report 2021 however at least provides some hints as to how states can avoid impairing critical infrastructure of other states. It suggested that states 'put in place relevant policy and legislative measures' to ensure compliance with the norm.[17] Such measures, seemingly akin to an impact assessment standard[18], can however so far only be considered best practice.

Aside from critical infrastructure, states have highlighted the negative obligation not to conduct harmful operation with regard to several other categories of significant cyber harm, without however providing substantially more nuance as to which activities are prohibited. Resembling the restrictive formulation of the critical infrastructure duty para. 13 lit.k of the UN GGE Report 2015 requires states not to 'conduct or knowingly support activity to harm the information systems of the authorized emergency response teams'.[19] The norm may be read as restricting potential hack-back operations. States have also highlighted the negative obligation

15 On the increasing concern over harm against governmental institutions see chapter 3.C.IV.3.

16 Ibid.

17 UN GGE Report 2021, para. 46.

18 Peter Stockburger, 'From Grey Zone to Customary International Law: How Adopting the Precautionary Principle May Help Crystallize the Due Diligence Principle in Cyberspace', in Tomáš Minárik/Raik Jakschis/Lauri Lindström (eds.) *10th International Conference on Cyber Conflict CyCon X: Maximising Effects 2018* (NATO CCD COE 2018), 245–262, at 260.

19 UN GGE Report 2015, para. 13k; on the establishment of a CERT as a due diligence requirement see below chapter 4.D.IV; see also the endorsement by Canada, Canada's Proposal for the Report of the 2019–20 United Nations Open-Ended Working Group

not to impair the public core of the internet.[20] Spain and the GCSC recommendations for example asserted that states should not launch attacks on the internet itself.[21] In a similar vein, Canada asserted in the UN OEWG that states should consider the potentially harmful effects of their activities on the 'technical infrastructure essential to the general availability or integrity of the Internet'.[22] States did not specify when an impairment of the public core would occur but it can be assumed that at least the tampering with the main protocols, potentially also via attacks on the integrity of the supply chain[23], and impairing fibre-optic or copper cables[24], would violate the negative prohibitive dimension of the harm prevention rule.

II. States' negative obligations regarding all categories of significant cyber harm

For the sake of comprehensiveness, it is to be noted that beyond the above-mentioned forms of significant cyber harm the negative prohibitive dimension of the harm prevention rule also requires states to abstain from all other forms of significant cyber harm, e.g. acts amounting to internationally wrongful acts.[25] It furthermore needs to be noted that regarding the prohibitive negative dimension the attribution problem will recur.[26] The notoriety of this problem will regularly limit the efficacy of grasping malicious state-sponsored cyber operations under the negative prohibitive dimension of the harm prevention rule.

---

on "Developments in the Field of Information and Telecommunications in the Context of International Security", 2019, p. 1.

20 On harm to the public core of the internet as a distinct category of significant harm see above chapter 3.C.III.

21 Spain highlighted attack on the internet itself as one of the main threats in cyberspace, Spain, Submission to the United Nations General Assembly Resolution A/RES/64/129/Add.1, 8 July 2009, p. 10; see also GCSC, Final Report 2019, Proposed Norms, p. 21, Norm 1: 'State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace'.

22 UN OEWG Chair's Summary, A/AC.290/2021/CRP.3, 10 March 2021, p. 13.

23 See below chapter 4.C.V.5.

24 See on the meaning of the public core of the internet chapter 3.C.III.

25 See chapter 3.B.

26 On the notorious attribution problem in cyberspace see the Introduction.

B. Required standard for due diligence under the harm prevention rule in cyberspace

Regarding the positive preventive dimension of the harm prevention rule the required standard for discharging the obligation is due diligence.[27] While due diligence is defined abstractly as a 'measure of prudence, activity, or assiduity, as is properly to be expected from, and ordinarily exercised by, a reasonable and prudent [person or enterprise] under the particular circumstances'[28] it is inherently difficult to determine what due diligence requires *in concreto*.[29] States have repeatedly called for guidance in implementing the rule.[30] The most common standard for discharging due diligence is the standard of reasonableness.[31] This standard has been endorsed by states in cyberspace, e.g. by Australia, Estonia or the Netherlands.[32]

27 See chapter 2.A.V.

28 ILA Study Group on Due Diligence in International Law, First Report, 7 March 2014, p. 19; UN Human Rights Office of the High Commissioner, *The Corporate Responsibility to Respect Human Rights: An Interpretive Guide* (United Nations 2012), p. 4.

29 Highlighting the lack of clear a content of due diligence Harriet Moynihan, 'The Application of International Law to State Cyberattacks Sovereignty and Non-intervention', *Chatham House – Research Paper*, 2019, para. 75; on the need for specification Liisi Adamson, 'Recommendation 13c', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 49–75, at 75, para. 40.

30 UN OEWG, Pre-draft Report 2020, para. 37: UN OEWG, Zero Draft 2021, paras. 32, 48; Canada, Canada's Proposal for the Report of the 2019–20 United Nations Open-Ended Working Group on "Developments in the Field of Information and Telecommunications in the Context of International Security, 2020, p. 2; Netherlands, The Kingdom of the Netherlands' response to the pre-draft report of the OEWG, 2020, p. 4; Republic of Korea, Report, 14 April 2020, p. 5. Joint comments from the EU and its Member States on the initial 'pre-draft' report of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security, 2020, p. 11, para. 32.

31 ILA Study Group on Due Diligence in International Law, Second Report, July 2016, p. 8; Anne Peters/Heike Krieger/Leonhard Kreuzer, 'Dissecting the Leitmotif of Current Accountability Debates: Due Diligence in the International Legal Order', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 1–19, 5; The ILC seemingly even equates due diligence with reasonability when it refers to the necessity of a 'reasonable standard of care or due diligence', ILC, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, UN General Assembly, Supp. No. 10, UN Doc A/56/10 (2001), commentary to article 3, para. 10.

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

Reasonable diligence is defined as 'such diligence as can reasonably be expected if all circumstances and conditions of the case are taken into consideration'.[33] The UN GGE Reports 2021, Canada and the UK referred to taking 'appropriate and reasonably available and feasible measures'.[34]

For assessing reasonableness in a specific case countervailing legal interests need to be taken into account. As asserted by the CoE Report 2011 the 'degree of care should be proportional to the degree of risk involved and the consequences incurred'.[35] Countervailing interests of particular importance in cyberspace are human rights obligations.[36] Risks for human rights

---

p. 91; Kersti Kaljulaid, President of the Republic at the opening of CyCon 2019, 29 May 2019, available at: https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-openingof-cycon-2019/index.html; Netherlands, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, Appendix, International Law in Cyberspace, p. 4.

33 Lassa Oppenheim, *International Law. A Treatise, Vol. II, War and Neutrality* (New York/Bombay: Longmans, Green and Co. 1906), 393.; see also Robert Sprague/Sean Valentine, 'Due Diligence', *Encyclopædia Britannica*, 4 October 2018, available at: https://www.britannica.com/topic/due-diligence.: 'The effort is measured by the circumstances under which it is applied, with the expectation that it will be conducted with a level of reasonableness and prudence appropriate for the particular circumstances.'

34 UN GGE Report 2021, para. 29: similar United Kingdom, UN GGE on Advancing Responsible State Behaviour in Cyberspace, Statement, May 2021, para. 12: 'The UK recognises the importance of States taking appropriate, reasonably available, and practicable steps within their capacities to address activities that are acknowledged to be harmful in order to enhance the stability of cyberspace in the interest of all States'; Canada, Canada's implementation of the 2015 GGE norms, Proposed norm guidance, 2019, p. 2.

35 CoE, Steering Committee on the Media and New Communication Services (CDMC), Explanatory Memorandum to the draft Recommendation CM/Rec(2011) of the Committee of Ministers to member states on the protection and promotion of Internet's universality, integrity and openness, CM(2011)115-add1 24 August 2011, para. 82; see also ILC Draft Articles on Prevention 2001 (n. 31), commentaries to art. 3, p. 154, para. 11:'The standard of due diligence against which the conduct of the State of origin should be examined is that which is generally considered to be appropriate and proportional to the degree of risk of transboundary harm in the particular instance', p. 155, para. 18: 'The required degree of care is proportional to the degree of hazard involved'.

36 UN GGE Report 2015, para. 13 lit.e: 'States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.' On the relevance of individual rights with regard to diligence measures see already Pufendorf

have for example been the reason for legitimate concerns regarding an over-extensive interpretation of due diligence in cyberspace.[37] Determining the requirements of due diligence is overall a context-dependent flexible assessment. As it is persistently difficult to determine the requirements of due diligence *ex ante*[38] a close look on a case-by-case basis is necessary to fill the abstract legal criteria with cyber-specific meaning.

I. Due diligence as a capacity-dependent binding obligation of conduct

The duty to exercise due diligence to prevent harm is an obligation of conduct.[39] It is not required that states deliver the absence of harm as a particular result. As long as a state has exercised due diligence it will not be held accountable, even if harm occurs. It is nevertheless important to note that the obligation to exercise due diligence under the harm prevention rule is a binding obligation and that its violation will entail international legal responsibility.[40] Furthermore, it is an *international* legal standard – states can hence not excuse negligence by pointing towards *diligentia in quam suis*.[41] If taking certain diligence measures is beyond a state's capacity it will however generally not be held accountable.[42] Due to greatly diverging technological ICT capacities this aspect is particularly relevant in cyberspace.[43] Yet, an objective international minimum standard of due diligence is binding for all states.[44] In the interconnected cyberspace it seems particularly important to focus on avoiding standards below this minimum

---

as depicted in Maria Monnheimer, *Due Diligence Obligations in International Human Rights Law* (Cambridge: Cambridge University Press 2021), 80.

37 See chapter 2.E.II.1.

38 Peters/Krieger/Kreuzer, 'Dissecting the Leitmotif' 2020 (n. 31), 12.

39 See chapter 2.A.V.1; see also ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment of 26 February 2007, ICJ Reports 2007, p. 43, para. 430.

40 Peters/ Krieger/Kreuzer, 'Dissecting the Leitmotif' 2020 (n. 31), 6.

41 Max Huber, *British Claims in the Spanish Zone of Morocco*, Award of 13 May 1925, vol. II, UNRIAA, 615, 644.

42 ILA, Second Report (n. 31), p. 3; implicitly affirming the relevance of a state's capacity for discharging the duty to prevent ICJ, *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgment of 24 May 1980, ICJ Reports 1980, p. 3, 32, para. 63.

43 CoE, 'Explanatory Memorandum' (n. 35), para. 77; Monnheimer, 'Due Diligence ' 2021 (n. 36), 123, 124.

44 ILC Draft Articles on Prevention 2001 (n. 31), commentaries to art. 3, p. 155, para. 17.

bottom line.[45] Above the international minimum standard higher standards may be binding on states with higher capacities. While such divergences may seem prima facie inequitable it is widely accepted in international law that diverging capacities can lead to divergent standards of accountability.[46] Hence, if a state has a certain technical apparatus, for example for intercepting communications or for shutting down servers from which harmful activities emanate, due diligence requires the respective state to use it and a state will entail international legal responsibility if it (negligently) fails to do so.[47]

II. Due diligence vs. 'soft' best practice standards

In contrast to binding standards of diligence *best practice* standards are best practices in the very meaning of the word and do not constitute binding law. They are rather soft standards to aspire to. Over time, soft best practice may harden to a binding customary standard or be incorporated into treaty law.[48] They can hereby be helpful 'halfway points'[49] in the law formation process. Informal and formal can overlap and co-exist complementarily and

45 On the relevance of the bottom line of due diligence Peters/Krieger/Kreuzer, 'Dissecting the Leitmotif' 2020 (n. 31), 12: 'The requirements of due diligence are context-dependent, often highly discretionary. In practice, the 'optimal' diligence probably never plays a role. When a dispute arises, the question is rather the bottom line. Court or other monitoring bodies will have to decide when due diligence was breached, not what would have been best'. exemplarily expressing such a bottom line *Mexico-US General Claims Commission, L. F. H. Neer and Pauline Neer (USA v. United Mexican States)*, 15 October 1926, vol. IV, UNRIAA, 60, para. 4: '[the] treatment of an alien, in order to constitute an international delinquency, should amount to an outrage, to bad faith, to wilful neglect of duty, or to an insufficiency of governmental action so far short of international standards that every reasonable and impartial man would readily recognize its insufficiency.'

46 In international climate change law, the notion of common but differentiated responsibilities e.g. informs the required standard of states' due diligence, see Lavanya Rajamani, 'Due Diligence in International Change Law', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 163–180, at 174.

47 François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press 2020), 362.

48 Hollin Dickerson, 'Best Practices', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2010), para. 21.

49 Ibid., para. 22.

interact.[50] Even if soft best practice norms do not harden to binding law they may nevertheless have a significant stabilizing effect as they induce norm adherence and cooperative state action even without, or potentially facilitated, by their non-binding character.[51] There is hence an inherent merit in collecting and assessing best practice standards. Several actors have called on a global repository of best practices regarding the implementation of the norms on responsible state behavior in the UN GGE Reports. Norway and Estonia have for example supported the establishment of a global repository to avoid fragmentation of international standards[52] and also the NAM has expressed its support.[53]

Different from soft law best practices are mere CMBs. CBMs are frequently mentioned in the UN GGE and UN OEWG Reports.[54] As the term indicates such measures aim to build confidence and to incentivize a

50 Mark A. Pollack/Gregory C. Shaffer, 'The Interaction of Formal and Informal International Lawmaking, in Joost Pauwelyn/Ramses A. Wessel/Jan Wouters (eds), *Informal International Lawmaking* (Oxford: Oxford University Press 2012) 241–270, at 242: 'More specifically, we suggest that formal and informal laws and lawmaking processes are likely to interact in a complementary fashion where distributive conflict is low, while informal and formal laws and lawmaking forums are likely to interact in competitive, antagonistic ways where distributive conflict among States is high.'

51 Dinah L. Shelton, 'Law, Non-Law and the Problem of "Soft Law"', in Dina L. Shelton (ed.) *Commitment and Compliance: The Role of Non-Binding Norms in the International Legal System* (Oxford: Oxford University Press 2000), 1–20, at 2.

52 Comments by the Norwegian Delegation on the "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security, p. 2; see also Microsoft, Submission to OEWG Draft Substantive Report, p. 2; Estonia's comments to the "Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security", 16 April 2020, paras. 1, 13, 18; China voiced concerns regarding a repository as expanding divisions and undermining trust China's Contribution to the Initial Pre-Draft of OEWG Report, p. 5.

53 Non-Aligned Movement, NAM Working Paper for the Second Substantive Session of the Open-ended Working Group on developments in the Field of Information and Telecommunications in the Context of International Security (UN OEWG), January 2021, p. 1: 'Member States should be encouraged to compile and streamline the information that they presented on their implementation of international rules and the relevant proposed repository (…)'; the establishment of a repository is mentioned as a potential CBM in the UN OEWG Chair's Summary, A/AC.290/2021/CRP.3, 10 March 2021, p. 6, para. 31.

54 UN GGE Report 2021, paras. 74–86; UN GGE Report 2015, paras. 16–18; United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013 (UN GGE Report 2013), paras. 26–29; UN OEWG Revised pre-draft, p. 8, paras. UN OEWG Final Report 2021 paras. 41–53.

cooperative dialogue.[55] Although they may partially overlap with soft law practices CBMs are preferably distinguished. Soft law still stirs normative aspirations and expectations. By contrast, the emphasis of CBMs on 'confidence' building suggests to allocate them on the level of international comity.[56]

III. Systematic interpretation of due diligence requirements in cyberspace

The international legal standard of due diligence is not to be assessed in isolation but with a view to existing standards of diligent behaviour stipulated by other primary rules of international law. The *South China Sea Arbitration* is an example of such a contextual interpretation of due diligence. In this case, the tribunal specified due diligence requirements by taking UNCLOS and international environmental law more generally into account.[57] The underlying rationale for interpreting due diligence in such a contextual manner is that standards should be interpreted systemically within the context of other rules of law.[58] The ICJ expressed this rationale well in its Advisory Opinion on the *Interpretation of Agreement* in 1980. It stated:

55 UN GGE Report 2021, para. 74: 'The Group notes that by fostering trust, cooperation, transparency and predictability, confidencebuilding measures (CBMs) can promote stability and help to reduce the risk of misunderstanding, escalation and conflict.'

56 Jörn Axel Kämmerer, 'Comity', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2020), para. 1.

57 Permanent Court of Arbitration, South China Sea Arbitration, Philippines v. China, Award of 12 July 2016, PCA Case No 2013–19, ICGJ p. 373–374, para. 941; on this integrative reading of due diligence Jutta Brunnée, 'Procedure and Substance in International Environmental Law', *Recueil des Cours de l'Académie de Droit International de la Haye* 405 (2020) 77–240, at 160.

58 On the desirability of coherence in the international legal order, see Anne Peters, 'The Refinement of International Law: From Fragmentation to Regime Interaction and Politicization', *International Journal of Constitutional Law* 15 (2017), 671–704; ILC, Report of the Study Group, finalized by Martti Koskenniemi, Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law, A/CN.4/L.682, 13 April 2006, p. 216, para. 430: '(…) treaties should be interpreted "in the context of the rules of international law" (…) this principle was taken for granted. Nobody challenged the idea that treaties were to be read in the context of their normative environment.' The contextual interpretation of norms in international law has also been termed as 'regime interaction', see Nele Matz-Lück, 'Norm Interpretation across International Regimes: Competences and Legitimacy', in Margaret A. Young (ed.), *Regime Interaction in International Law* –

> '[A] rule of international law, whether customary or conventional, does not operate in a vacuum; it operates in relation to facts and in the context of a wider framework of legal rules of which it forms only a part.'[59]

Similarly, the ICJ asserted in its *Namibia* Advisory Opinion:

> '[I]nterpretation and application of existing international instruments to ICTs "within the framework of the entire legal system prevailing at the time of such interpretation"'.[60]

Interpreting due diligence requirements in cyberspace hence needs to take other rules and standards of international law into account. The Czech Republic has explicitly recognized this principle for the interpretation of international law in cyberspace.[61] Also commentators have highlighted the need to interpret due diligence in light of other international legal rules and standards. The Tallinn Manual has for example been criticized for failing to take other legal regimes sufficiently into account, in particular human rights law.[62]

IV. The relevance of the duty to protect under international human rights law

Especially the duty to protect human rights may influence the required standard under the harm prevention rule. Commentators have highlighted

---

Facing Fragmentation (Cambridge: Cambridge University Press 2012), 201–234, at 209f.

59 ICJ, *Interpretation of the Agreement of 25 March 1951 Between the WHO and Egypt*, Advisory Opinion of 20 December 1980, ICJ Reports 1980, p. 73, 76, para. 10.

60 ICJ, *Legal Consequences for States of the Continued Presence of South Africa in Namibia notwithstanding Security Council Resolution 276 (1970)*, Advisory Opinion of 21 June 1971, ICJ Reports 1971, p. 16, 54, para. 118.

61 Czech Republic, Comments submitted by the Czech Republic in reaction to the initial "pre-draft" report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security, March/April 2020, para. II.iii): 'In particular, the UN OEWG could highlight the following principles, which should guide the applicability of international law in the context of ICTs: (…) interpretation and application of existing international instruments to ICTs "within the framework of the entire legal system prevailing at the time of such interpretation".

62 Antal Berkes, 'Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control', *Israel Law Review* 52 (2019) 197–231, at 219.

that the 'patchwork' of human rights obligations plays an important role for stabilizing cyberspace.[63] The particular importance of due diligence requirements under the duty to protect in international human rights law warrants a substantive depiction of international human rights law and its relation to due diligence under the harm prevention rule in cyberspace.

Unter international human rights law states have a due diligence duty to protect individuals from risks of cyber harm if the risk of harm reaches a certain significance threshold.[64] While a report of the International Law Association in 2016 had still asserted that states do not yet assume a duty to protect in cyberspace[65] states have increasingly recognized this duty in recent years[66], in particular in light of cyber incidents during the COVID-pandemic.[67] The relevance of human rights law for the harm prevention rule can already be seen in the relevance of harm to human rights for assessing the significance threshold – which inter alia takes into account

63 Antonio Coco/Talita de Souza Dias, '"Cyber Due Diligence"': A Patchwork of Protective Obligations in International Law', *European Journal of International Law* 32 (2021), 771–805, at 804: 'Thus, in a way, there is a patchwork of different but overlapping protective obligations requiring diligent behaviour in cyberspace'; affirming the applicability of international human rights law in cyberspace e.g. UN Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet, A/HRC/RES/26/13, 14 July 2014.

64 IACtHR, Case of Velásquez-Rodríguez v. Honduras, Judgment of 29 July 1988, Series C No. 4, para. 172;, ECtHR, *Case of Osman v. the United Kingdom*, Grand Chamber Judgment of 28 October 1998, Application No. 23452/94, para. 116; Björnstjern Baade, 'Due Diligence and the Duty to Protect Human Rights', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 92–108.

65 International Law Association, *Study Group on Cybersecurity, Terrorism, and International Law,* 31 July 2016, para. 71.

66 Australia, 'Cyber Engagement Strategy' 2019 (n. 32), p. 3: 'States have obligations to protect relevant human rights of individuals under their jurisdiction, including the right to privacy, where those rights are exercised or realised through or in cyberspace'; seemingly hinting also at the protective dimension under human rights law Pre-Draft Report of the UN OEWG – ICT Comments by Austria, 31 March 2020,p. 3: 'sovereignty entails rights and obligations for States, in particular with regard to the observance of human rights and fundamental freedoms, including on data protection and privacy, freedom of expression, and freedom of information.'

67 See e.g. UN GGE Report 2021, para. 71b: 'States exercise jurisdiction over the ICT infrastructure within their territory by, inter alia, setting policy and law and establishing the necessary mechanisms to protect ICT infrastructure on their territory from ICT-related threats'.

whether persons have been injured.[68] Furthermore, the due diligence duty to protect under human rights law carries several structural and doctrinal similarities with due diligence under the harm prevention rule, making its requirements particularly informative for the required standard of due diligence under the harm prevention rule. First, due diligence is also triggered by the risk of harm of a certain severity.[69] Second, once a risk of harm is objectively foreseeable[70] due diligence is triggered by the existence of a general risk to an unidentified number of individuals.[71] Third, the requirements of due diligence under the duty to protect are also assessed via a context-dependent reasonability standard.[72] States enjoy a wide margin of appreciation in fulfilling their positive obligations[73] and are only required to exercise best efforts.[74] The determination of the required due diligence furthermore takes a state's capacity and budgetary constraints into account to avoid intrusive 'micromanaging' of national institutions[75]

68 ILC Draft Articles on Prevention 2001 (n. 31), art. 2b: 'Harm" means harm caused to persons, property or the environment'.

69 ECtHR, *Case of Denisov v. Ukraine,* Grand Chamber Judgment of 25 September 2018, Application no.76639/11, para. 110.

70 Speculative risks do not suffice Baade, 'The Duty to Protect' 2020 (n. 64), Laurens Lavrysen, *Human Rights in a Positive State* (Intersentia 2017), at 131–137.

71 The IACtHR has e.g. in this regard distinguished between general and 'strict' due diligence. IACtHR, *Case of González et al. (Cotton Field) v. Mexico,* Judgment of 16 November 2009, Series C No. 205, paras 281–283; see Baade, 'The Duty to Protect' 2020 (n. 64), 98; also pointing out that the character or remoteness of the risk influences which measures need to be taken, e.g protective operational measures and providing general protection Vladislava Stoyanova, 'Fault, Knowledge and Risk Within the Framework of Positive Obligations under the European Convention on Human Rights', *Leiden Journal of International Law* 33 (2020), 601–620, 606; affirming this for the cyber context see Monnheimer, 'Due Diligence ' 2021 (n. 36), 200: 'Knowledge of [a] broad and general risk should trigger preventive obligations.'

72 ECtHR, 'Osman' (n. 64), para. 151; IACtHR, 'Velasquez Rodriguez v. Honduras' (n. 64), para 167; Baade, 'The Duty to Protect' 2020 (n. 64), 97.

73 Heike Krieger, 'Positive Verpflichtungen unter der EMRK: Unentbehrliches Element einer gemeineuropäischen Grundrechtsdogmatik, leeres Versprechen oder Grenze der Justiziabilität?', *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* 74 (2014), 187–213.

74 Helmut Philipp Aust, 'Spionage im Zeitalter von Big Data – Globale Überwachung und der Schutz der Privatsphäre im Völkerrecht', *Archiv des Völkerrechts* 52 (2014), 375–406, at 402.

75 Baade, 'The Duty to Protect' 2020 (n. 64), 101.

or a disproportionate burden.[76] Hence, several structural similarities to due diligence requirements under the harm prevention rule exist.[77]

It is however important to note that the overlap of due diligence under the harm prevention rule and due diligence for human rights protection is only partial. The main difference between both regimes lies in its protective scope. While the harm prevention rule is predominantly protecting against cyber harm manifesting extraterritorially the duty to protect under human rights law primarily aims to prevent risks of harm manifesting on a state's own territory. It only exceptionally requires to prevent risks of harm manifesting on the territory of another state.[78] Furthermore, the balancing process deviates structurally. In international human rights law proportionality balances the interests of protected individuals versus the interests of individuals affected by protective measures.[79] This is 'value-laden'[80] and structurally different from the harm prevention rule which balances the competing interests of sovereign states.

Regarding the stringency of due diligence requirements this leads to ambiguous results. On the one hand, due diligence requirements under human

76 ECtHR, *Case of Nicolae Virgiliu Tănase v. Romania*, Judgment of 25 June 2019, Application No. 41720/13, para. 136; see also Coco/Dias, 'Cyber Due Diligence' 2021 (n.63), 799; UN Human Rights Committee, General Comment No. 36 on article 6 of the International Covenant on Civil and Political Rights, on the right to life, 30 October 2018, CCPR/C/GC/36, para. 21.

77 On due diligence requirements under the harm prevention rule see above chapter 4.B.I, II.

78 Arguing for a functional approach Yuval Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law', *Law & Ethics of Human Rights* 7 (2013) 47; UN Human Rights Committee, 'General Comment 36' (n. 76), para. 63; see also Coco/Dias, 'Cyber Due Diligence' 2021 (n.63), 798; on a duty to regulate corporations with extraterritorial activities Elif Askin, 'Economic and Social Rights, Extraterritorial Application', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2019), paras. 33f.

79 Heike Krieger/Anne Peters, 'Due Diligence and Structural Change in the International Legal Order', in Heike Krieger/Anne Peters/Leonhard Kreuzer, *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 351–390, at 370: '[T]he elements of the balancing process differ from those under due diligence in general international law. In human rights law, balancing may involve conflicting public interests and the human rights of other individuals. Protection against harmful activities of non-state actors in itself impacts on human rights of those others.'

80 Ibid.

rights law are arguably more demanding[81] than due diligence requirements under the harm prevention rule and may require a specific result in specific cases and hereby go beyond mere best efforts requirements.[82] On the other hand, due to the more complex balancing process, the margin of appreciation in international human rights law is an important tool for respecting democratic self-government and hence not to be interpreted restrictively.[83]

The 'family resemblance'[84] of due diligence under both regimes nevertheless requires to take human rights due diligence obligations into account when assessing due diligence requirements under the harm prevention rule, mainly for two reasons. First, taking the due diligence duty to protect into account is important to avoid fragmentation of international standards of diligence.[85] Second, taking protective duties under human rights law into account complementarily allocates risk accountability in the case of harm. If a victim state fails to diligently protect individuals under its jurisdiction against cyber harm which emanates from the territory of another state this negligence may be considered complementary contribution to the occurrence of cyber harm. As a consequence, restitution and compensation claims under the harm prevention rule may be reduced.[86]

Beyond human rights law other legal regimes, such as anti-terrorism law, telecommunications law, technical standards[87], as well as subsequent state practice regarding cybercrime treaties, may inform the required standard of 'reasonability' regarding cyber due diligence. The study will take such standards into account where appropriate.

81 Marko Milanovic/Michael Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations during a Pandemic', *Journal of National Security Law & Policy* 11 (2020), 247–284, at 281–282.

82 Krieger/Peters, 'Structural Change' 2020 (n. 79), 370.

83 Ibid.; Björnstjern Baade, *Der Europäische Gerichtshof für Menschenrechte als Diskurswächter* (Springer 2017).

84 Krieger/Peters, 'Structural Change' 2020 (n. 79), 370.

85 On the need for a systematic interpretation of due diligence which takes other rules of international law into account see above chapter 4.B.III.

86 See chapter 5.B.I.

87 UK Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015.UK, September 2019, p. 4: 'We also look to develop industry standards on security of technology, which help build cyber resilience globally. We continue to be active in the international standards space.'

V. Categories of due diligence measures

As pointed out elsewhere[88] two broad categories of diligence requirements can be discerned: Procedural due diligence obligations, and measures of institutional capacity-building. Procedural obligations are for example duties to report[89], to warn, to cooperate[90], or to assist.[91] Procedural obligations are a core part of risk management in the international legal order[92] and may be particularly important with regard to imminent and ongoing cyber incidents.

By contrast, measures of institutional capacity-building strengthen emergency preparedness[93] and resilience by providing organizational structures for risk prevention and mitigation[94], e.g. through legislative and administrative safeguard measures. Such measures are frequently instrumental for discharging procedural due diligence obligations.[95] Having for example a national computer emergency response team (CERT) can be a pre-requirement to discharge procedural due diligence obligations to assist or warn in cases of ongoing cyber operations. Similarly, it is also necessary to enact cybercrime legislation in order to diligently prosecute cyber criminals.

88 Anne Peters/Heike Krieger/Leonhard Kreuzer, 'Due diligence: the risky risk management tool in international law', Cambridge Journal of International Law 9 (2020), 121–136, 121; for an alternative framing as obligation of result (to have sufficient legislation and administrative apparatus) and an obligation of conduct (to use that capacity diligently) see Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', *Journal of Conflict & Security Law* 21 (2016), 429–453.

89 For example to report tax under the Organisation for Economic Co-operation and Development (OECD) framework; or the duty to 'prepare, communicate and maintain' successive nationally determined contributions' on greenhouse gas mitigation under art. 4.2 of the Paris Agreement in international climate change law, Rajamani, 'Climate Change Law' 2020 (n. 46), 168.

90 ILC Draft Articles on Prevention 2001 (n. 31), art. 4.

91 Highlighting the importance of procedural obligations for discharging due diligence duties of diligent harm prevention Phoebe Okowa, 'Procedural Obligations in International Environmental Agreements', *British Yearbook of International Law* 67 (1997), 275–336, at 332.

92 On the trend towards proceduralisation Peters/Krieger/Kreuzer, 'Risky risk management' 2020 (n. 88), 135.

93 ILA, 'Cybersecurity and Terrorism' 2016 (n. 65), para. 247.

94 ILC Draft Articles on Prevention 2001 (n. 31), art. 5 refers to 'necessary legislative, administrative or other action including the establishment of suitable monitoring mechanisms to implement the provisions of the present articles'.

95 On the interrelation of procedural due diligence obligations and such safeguard measures Coco/Dias, 'Cyber Due Diligence' 2021 (n.63), 804.

In the cyber context, the ITU has suggested an alternative categorisation of diligence measures and has distinguished between legal measures; technical and procedural measures; organizational structures; capacity building; international cooperation.[96] While this categorization provides an illustrative overview it mixes clearly non-binding measures, such as capacity building, with potentially legally binding diligence measures (e.g. legal measures). For the sake of greater legal clarity as to the bindingness of due diligence obligations this study will follow the distinction between procedural due diligence measures and measures of institutional capacity-building.

C. Procedural due diligence measures

I. Duty to cooperate

The necessity of international cooperation is repeatedly stressed throughout discussions in the UN GGE and UN OEWG. In the context of the harm prevention rule, this raises the question whether cooperation is a procedural due diligence requirement.

96 TU Global Cybersecurity Agenda (GCA), High-Level Experts Group (HLEG), Report of the Chairman of the HLEG (2008), available at: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx, p. 4.

1. Cooperation in international law

Inter-state cooperation is one of the purposes of the UN[97] and is essential for the maintenance of international peace and security.[98] The *Declaration on Friendly Relations and Co-Operation*[99] asserts that

> '[s]tates have the duty to co-operate with one another, irrespective of the differences in their political, economic and social systems, in the various spheres of international relations, in order to maintain international peace and security and to promote international economic stability and progress (…)'[100]

The term 'law of cooperation' (as opposed to the 'law of coordination')[101] hence expresses the necessity of coordinated state action to achieve various shared goals in modern international law. Cooperation is linked to the bona

97 Charter of the United Nations, 24 October 1945, 1 UNTS XVI, art. 1 (3): 'To achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion (…)'.

98 Ibid., art. 11 (1):' The General Assembly may consider the general principles of cooperation in the maintenance of international peace and security (…)'; art. 55, 56: '(…) United Nations shall promote: a. higher standards of living, full employment, and conditions of economic and social progress and development; b. solutions of international economic, social, health, and related problems; and international cultural and educational cooperation; and c. universal respect for, and observance of, human rights and fundamental freedoms for all without distinction as to race, sex, language, or religion' art. 56: 'All Members pledge themselves to take joint and separate action in co-operation with the Organization for the achievement of the purposes set forth in Article 55.'

99 The Declaration reflects customary international law see ICJ, *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion of 22 July 2010*, ICJ Reports 2010, p. 403, para. 80; Helen Keller, 'Friendly Relations Declaration (1970)', in Anne Peters (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2021), paras. 39, 40; Zine Homburger, 'Recommendation 13a', in Eneken Tikk (ed.) *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary,* (United Nations Office for Disarmament Affairs 2017), 9–25, at 12, para. 8.

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

101 On the term see the seminal work of Wolfgang Friedman*, The Changing Structure of International Law* (London: Stevens 1964); on both terms as 'different techniques of legal regulation' Rüdiger Wolfrum, 'International Law of Cooperation', in Rüdiger

fide principle in Art. 2 (2) UN Charter and hence a core normative expectation inherent in international relations.[102] In various areas of international law binding duties to cooperate can be found, for example in international human rights law[103], in anti-terrorism law[104] or with regard sustainable development.[105]

2. Cooperation and due diligence

In the context of the harm prevention rule, cooperation is an essential element for discharging due diligence. Art. 4 of the ILC Draft Prevention Articles asserts a duty of cooperation with regard to the prevention of transboundary harm:

> 'States concerned shall cooperate in good faith (…) in preventing significant transboundary harm or at any event in minimizing the risk thereof'.[106]

Also the preamble, as well as ILC Draft Principles on the Allocation of Loss, reiterate a 'duty of cooperation' with regard to the prevention of transboundary harm.[107] The ILC Draft Articles on Prevention further out-

Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2010), paras 39–65.

102 On the link between cooperation and good faith ICJ, *Nuclear Tests (Australia v. France)*, Judgment of 20 December 1974, ICJ Reports 1974, p. 268, para. 46: 'One of the basic principles governing the creation and performance of legal obligations, whatever their source, is the principle of good faith. Trust and confidence are inherent in international co-operation, in particular in an age when this co-operation in many fields is becoming increasingly essential.'

103 International Covenant on Economic, Social and Cultural Rights in the context of business activities, E/C.12/GC/24, 10 August 2017, art. 2 (1): 'Each State Party to the present Covenant undertakes to take steps, individually and through international assistance and co-operation (…) with a view to achieving progressively the full realization of the rights recognized in the present Covenant (…)'.

104 UN, Security Council, Resolution 1373, S/RES/1373, 28 September 2001.

105 United Nations, General Assembly, Rio Declaration on Environment and Development, A/CONF.151/26, 13 June 1992, Rev.1; Principle 5: 'States and people shall cooperate in good faith and in a spirit of partnership in the fulfilment of the principles embodied in this Declaration (…).

106 ILC Draft Articles on Prevention 2001 (n. 31), art. 4.

107 ILC Draft Articles on Prevention 2001 (n. 31), preamble: 'Recognizing the importance of promoting international cooperation'; ILC, Draft Principles on the Allocation of Loss in the case of Transboundary Harm arising out of Hazardous activities,

line that a general due diligence duty to cooperate for harm prevention may entail further specific cooperative obligations[108], for example a duty to notify[109] or to conduct a risk assessment.[110] This suggests that often specific 'sub'-duties that derive from a general duty of cooperation are relevant for complying with due diligence in practice. The ICJ *Pulp Mills* case is an example of the relevance of such procedural sub-duties. In this case the ICJ analysed the interrelation between procedural obligations to inform and notify and a general obligation to cooperate with regard to shared resources. It found that cooperation is a necessary element of diligent harm prevention and highlighted that procedural sub-duties to inform and notify are necessary to discharge the broader cooperation requirement.[111] Although the Court analysed a bilateral treaty it linked its analysis to customary international law, hence indicating the relevance of its findings also beyond the analysed treaty.[112] A general-specific relationship between specific 'sub'-duties to cooperate and a general duty to cooperate can also be found in other areas of international law in which a duty to cooperate exists. In international economic law, for example, a specific duty to notify about proposed regulatory measures with significant trade effects contributes to the broader aim of 'facilitating trade through regulatory cooperation' in this area.[113]

Report of the ILC on the Work of its Fifty-Eighth Session, A/61/10, 1 May-9 June and 3 July-11 August 2006, principle 8 (3): 'States should cooperate with each other to implement the present draft principles.'

108 ILC Draft Articles on Prevention 2001 (n. 31), commentaries to art. 4, p. 155, para. 1: 'The principle of cooperation between States is essential (…) to prevent significant transboundary harm (…) More specific forms of cooperation are stipulated in subsequent articles.'

109 ILC Draft Articles on Prevention 2001 (n. 31), art. 8: If the assessment (…) indicates a risk of causing significant transboundary harm, the State of origin shall provide the State likely to be affected with timely notification of the risk and the assessment and shall transmit to it the available technical and all other relevant information on which the assessment is based.'

110 ILC Draft Articles on Prevention 2001 (n. 31), art. 7: 'Any decision in respect of the authorization of an activity within the scope of the present articles shall, in particular, be based on an assessment of the possible transboundary harm caused by that activity, including any environmental impact assessment.'

111 ICJ, *Pulp Mills on the River Uruguay Case (Argentina v. Uruguay)*, Judgment of 20 April 2010, ICJ Reports 2010, p. 14, 45, para. 101, 102.

112 Ibid.

113 See WTO/OECD, Facilitating trade through regulatory cooperation – The case of the WTO's TBT/SPS Agreements and Committees (WTO/OECD 2019), p.22.

3. Cooperation in cyberspace

In cyberspace, cooperation is frequently mentioned in the UN GGE Reports and the reports of the UN OEWG. The Guidance to the UN GGE Report 2021 stated:

> '[I]t is the common aspiration and in the interest of all States to cooperate and work together to promote the use of ICTs for peaceful purposes and prevent conflict arising from their misuse.'[114]

In his foreword to the UN GGE Report 2015 the UN Secretary-General emphasized the necessity of international cooperation to increase cyber security, hereby highlighting the vital importance of cooperation in cyberspace:

> 'Making cyberspace stable and secure can be achieved only through international cooperation, and the foundation of this cooperation must be international law and the principles of the Charter of the United Nations.'[115]

The norms of responsible state behaviour begin with a norm on cooperation which further underlines the centrality of cooperation for diligent harm prevention in cyberspace:

> 'Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.'[116]

Also France has linked cooperation to discharging due diligence in cyberspace.[117] In a reading that concurs with the above-mentioned general-specific relationship between a general normative expectation of cooperation and specific cooperative sub-duties commentators have argued that cooperation, as asserted in para. 13 lit. a, underlies also all following norms of responsible state behaviour in para. 13 lit. b–k. The underlying reason is that all norms of responsible behaviour presuppose coordinated state ac-

114 UN GGE Report 2021, para. 19.
115 UN GGE Report 2015, Foreword.
116 UN GGE Report 2015, para. 13a.
117 France, Revue stratégique de cyberdéfense, 12 February 2018, p. 86.

tion.[118] In this vein, *de Busser* has distinguished *general* cooperation under para. 13 lit. a from *specific* forms of cooperation, for example cooperation against criminal and terrorist use of cyberspace which is addressed in para. 13 lit. d.[119] A further specific area of cooperation concerns the protection of critical infrastructure which is addressed in para. 13 lit. g, lit. h.[120]

That cooperation constitutes a broad normative aspiration that also reaches into the realm of non-binding normative aspirations can be seen in both the UN GGE and the UN OEWG Reports. In both, cooperation is frequently mentioned with regard to capacity-building and CBMs.[121] The UN GGE Report 2015 even entails an own section on 'international cooperation'[122] that is tellingly disjointed from the parts on international law (Part VI) and the norms of responsible state behaviour (Part III). Cooperation is hence used in cyberspace as a catch-all term for coordinated action between states, without necessarily carrying legal weight or suggesting a binding or soft law character.

This can also be seen in cooperation references in various bilateral, regional, both binding and non-binding agreements on cybersecurity. The regional cyber security agreement of the SCO refers to cooperation in its name[123] but falls short of stipulating specific cooperative obligations. Also

118 Homburger, 'Recommendation 13 a' 2017 (n. 99), p. 10, para. 2: 'It is the basic assumption that such transboundary threats cannot be prevented and mitigated by states acting individually (…)'; Adamson, 'Recommendation 13c' 2017 (n. 29), at 72, 73, para. 35.

119 Els de Busser, 'Recommendation 13d', in Enekken Tikk (ed.), Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary (United Nations Office for Disarmament Affairs 2017), 77–94, at 77, para. 2: 'Where recommendation (a) implies cooperation between states, the purpose is to maintain international peace and security. In this sense, the purpose of recommendation (a) is directly related to the United Nations Charter and the purposes of the United Nations expressed therein.1 In general, threats to international peace and security have a different scope than that of criminal offences and terrorist activities.

120 UN GGE Report, para. 13g, h; see also below chapter 4.D.III.

121 The UN OEWG Final Report refers numerously to cooperation but notably omits references in its part on international law or norms of responsible state behaviour; cooperation is frequently referred to in the context of CBMs and capacity building, see e.g paras. 54–67, paras. 41–53.

122 UN GGE Report 2015, International cooperation and assistance in ICT security and capacity-building, Part V, para. 19–23 (Part VI on international law, Part III on norms of responsible state behavior).

123 SCO, Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security, 2009.

the SCO draft code of 2015 entails only broad cooperative expectations.[124] Further non-binding MoU on cyber security often refer broadly to cooperation[125], for example to counter malicious cyber activities[126], cybercrime[127] or cyber terrorism[128], but they also similarly fall short of specificity or bindingness. Both the generality of the references to cooperation, as well as their lack of bindingness, hence currently prevents MoUs from providing sufficiently clear normative directions as to the content of a potential diligence duty to cooperate. Consequently, it is hard to deduce meaningful normative direction from these broad assertions with regard to the potential content of a general cooperation duty under the harm prevention rule.

4. Focus on specific cooperative duties preferable

Hence, it seems advisable to be cautious to refer to a self-standing duty to cooperate as a due diligence requirement in cyberspace.[129] Frequent, or even inflationary reference to cooperation as a catch-all term, as e.g. in

124 Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/69/723, para. 1: The purpose of the present code of conduct is to (…) (4) To cooperate in combating criminal and terrorist activities that use information and communications technologies (…); (12) To bolster bilateral, regional and international cooperation, (...) to enhance coordination among relevant international organizations'.

125 Japan – Israel, Memorandum of Cooperation in the Field of Cybersecurity Between the Ministry of Economy and Industry of the State of Israel: 'Recognizing the importance of cooperation in the field of cybersecurity between Entities of both countries in sharing knowledge and information, personnel exchange or cooperative research'.

126 ASEAN-EU Statement on Cybersecurity Cooperation, 1 August 2019, para. 2: 'We underscore our commitment to promote an open, secure, stable, accessible and peaceful information and communication technology (ICT) environment, consistent with applicable international and domestic laws. We intend to strengthen our cooperation on cyber issues.'

127 U.S.-China Cyber Agreement, 16 October 2015, 'both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory (…)'.

128 United Nations Office on Drugs and Crime (UN ODC), *The use of the Internet for terrorist purposes* (United Nations 2012), paras. 73–101.

129 Highlighting that states are unlikely to accept a general duty to cooperate Wolfrum, 'Cooperation' 2010 (n. 101), para. 40. Coco/Dias leave the question open whether a general duty to cooperate in cyberspace exists, see Talita de Souza Dias/Antonio

the UN GGE Reports, or the UN OEWG Reports[130], may weaken legal clarity. It also bears the risk that cooperation becomes a convenient term for states to pay lip-service to their shared responsibility for ensuring global cybersecurity, while simultaneously evading accountability.[131]

Both in customary international law, as well as in its cyber-specific recognition, cooperation is specified through more detailed obligations, such as obligations to inform, assist, or notify, or with regard to specific areas, such as with regard to cybercrime prosecution or critical infrastructure protection. With regard to the content of due diligence requirements it seems advisable to focus on such specific cooperative obligations.

II. Duty to take action against ongoing or imminent harmful operations

During the DDoS operation against Estonia in 2007 the Estonian government notified the Russian government that harmful cyber operations were emanating from Russian territory and asked the Russian government to assist in halting the operations. The Russian government however fell short of doing so. This example evokes the question whether a refusal to cooperatively stop or mitigate an imminent or ongoing malicious cyber operation emanating from a state's territory or in case of an emergency violates the obligation to exercise due diligence.

1. Duty to take action and due diligence

Due diligence to prevent significant harm may require a state to take action against ongoing or imminent harmful operations. Art. 5 of the ILC Draft Principles on the Allocation of Loss requires the state from which harm emanates to 'ensure that appropriate response measures are taken' upon

Coco, *Cyber due diligence in international law* (Print version: Oxford Institute for Ethics, Law and Armed Conflict 2021), 242.

130 UN GGE Report 2015, International cooperation and assistance in ICT security and capacity-building, Part V, paras. 19–23 (Part VI on international law, Part III on norms of responsible state behaviour); the Final report of the OEGW e.g. refers to cooperation 27 times, while largely falling short of stipulating legal rules and norms.

131 E.g. the SCO Information Cooperation h even refers to cooperation in its title but falls short of a defining any sufficiently differentiated means of cooperation, e.g. for mutual legal assistance, for securing evidence.

the occurrence of an incident.[132] The ICJ asserted due diligence duties to take action with regard to the mitigation of imminent or ongoing harm in the *Tehran Hostages*[133] case, as well as in the *Bosnia Genocide* case.[134] Furthermore, Art. 3 of the ILC Draft Prevention Articles requires states to 'prevent significant (…) harm or at any event minimize the risk thereof'.[135] The duty to take action against imminent or ongoing harmful operations can hence be considered a core requirement for discharging due diligence under the harm prevention rule.

2. Duty to take action in cyberspace

A large number of states have recognized that they may be required to take action against harmful cyber activities. Already in 2003 the UN General Assembly asserted that states should 'act in a timely and cooperative manner (…) to respond to security incidents'.[136] In a similar vein, para. 13 lit. h of the UN GGE Report 2015 asserts that

> 'States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty'.[137]

This formulation was reiterated by the UN General Assembly[138] and the UN GGE Report 2021.[139] While the first part of para. 13 lit. h seemingly asserts a general duty to respond to harmful cyber operations against the critical infrastructure of other states, regardless of whether such operations

132 Allocation of Loss, 2006 (n. 107), principle 5b.
133 ICJ, *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgment of 24 May 1980, ICJ Reports 1980, p. 3, 12, para. 18.
134 ICJ, 'Bosnia Genocide' 2007 (n. 39), para. 431.
135 ILC, Draft Articles on Prevention 2001 (n. 31), art. 3.
136 UN General Assembly Resolution A/RES/57/239, 31 January 2003, Annex, lit. c: 'Response. Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents. They should (…) implement procedures for rapid and effective cooperation to prevent, detect and respond to security incidents.'
137 UN GGE Report 2015, para. 13 lit. h.
138 UN General Assembly Res. A/C.1/73/L.27, 22 October 2018, para. 16.
139 UN GGE Report 2021, paras. 51–55.

emanate from a requested state's territory, the second part of para. 13 lit. h addresses the classical harm prevention rule constellation in which due diligence is required from a state from which harm is emanating. The assertion in para. 13 lit. h is limited to cyber operations against critical infrastructure. Yet, several assertions of states regarding a duty to take action do not mention such a limitation. South Korea for instance merely refers to a duty to respond with regard to cyber incidents.[140] Similarly, the Netherlands and Germany broadly refer to mitigation measures regarding 'cyber attack[s]'.[141] France highlighted critical infrastructure but also asserted a duty to assist beyond acts affecting critical infrastructure.[142] Also the Tallinn Manual which takes a restrictive stance on the requirements of due diligence[143] takes the view that states are required to 'stop' ongoing or imminent attacks, regardless of whether they are aimed at the critical infrastructure of other states, as long as they reach the threshold for triggering due diligence obligations.[144] Lastly, art. 10 (4) of the Additional Protocol II to the Budapest Convention on Cybercrime requires that in the case of an emergency the requested Party 'shall respond on a rapidly expedited basis.'[145]

140 Republic of Korea, 'Comments' 2020 (n. 30), p. 5: 'When an affected State notifies another State that ICT incidents has emanated from or involve the notified State's territory with qualified information, the notified State should, in accordance with international and domestic law and within their capacity, take all reasonable steps, within their territory, to cause these activities to cease, or to mitigate its consequences.'

141 Netherlands, 'International Law in Cyberspace' 2019 (n. 32), p. 4: 'If (…) a cyberattack is carried out against the Netherlands using servers in another country, the Netherlands may, on the basis of the due diligence principle, ask the other country to shut down the servers'. Germany, Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General, Submission by Germany, A/66/152, p. 10: 'State responsibility for cyberattacks launched from their territory when States do nothing to end such attacks despite being informed about them.'

142 France, Stratégie internationale de la France pour le numérique, 2017, p. 32: '(…) adopter un comportement coopératif vis-à-vis de pays victimes d'attaques émanant de son propre territoire, par application du principe de diligence requise, en particulier lorsque l'attaque vise une infrastructure critique'.

143 See chapter 2.A.V.2.

144 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 14), commentary to rule 7, p. 43, para. 2.

145 Council of Europe, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CETS No. 224, **17 November 2021,** art.10 (4): 'Once satisfied that an emergency exists and the other requirements for mutual assistance have been satisfied, the requested Party shall respond to the request on a rapidly expedited basis.' An emergency in the meaning

Overall, there is hence overwhelming evidence that states may be required to take action against imminent or ongoing cyber operations.[146] Notably, no state has rejected a duty to stop or mitigate ongoing harmful cyber operations. Furthermore, several states have directly linked a duty to take action to due diligence under the harm prevention rule, e.g. South Korea[147], France[148] and Australia.[149]

Due to the broad references to duties to take action regarding cyber incidents there is no principled objection that in principle *any* harmful cyber operation may trigger duties to stop or mitigate harmful operations. An overly broad interpretation of such a duty can be avoided by taking both the elements of knowledge and capacity into account. But more clarity regarding states' opinio iuris would be benefitial. The hint by France in the UN OEWG that a better understanding of due diligence may help '(…) putting a stop to potential major cyberattacks'[150] indicates this need for more clarity.

3. Knowledge

With regard to the knowledge criterion the regular scenario in which a state gains knowledge, also foreseen in the UN GGE Reports, is notification by another state.[151] Several states acknowledge such constellations as well.[152]

---

of Additional Protocol II exists when 'there is a significant and imminent risk to the life or safety of any natural person, art. 3 (2c).

146 Also asserting a duty to assist Henning Christian Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge: Cambridge University Press 2020), 159; GCSC, Final Report 2019, Proposed Norms, para. 8: 'Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.'

147 Republic of Korea, 'Comments' 2020 (n. 30), p. 5.

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

149 Australia's International Cyber Engagement Strategy, October 2017, p. 91: '[I]f a state is aware of an internationally wrongful act originating from or routed through its territory, and it has the ability to put an end to the harmful activity, that state should take reasonable steps to do so consistent with international law.'

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

151 Karine Bannelier/Theodore Christakis, *Prevention Reactions: The Role of States and Private Actors* (Les Cahiers de la Revue Défense Nationale 2017) 32.

152 Republic of Korea, 'Comments' 2020 (n. 30), p. 5; Netherlands, 'International Law in Cyberspace' 2019 (n. 32), p. 4.

The question if also a state through which a malicious cyber operation is routed – a so-called 'transit state'[153] – shoulders a due diligence obligation has been contentious.[154] A statement by South Korea in the UN OEWG refers to due diligence obligations to assist with regard to ICT activities which 'emanate *or involve*' a state's territory[155] – which suggests that also transit states may be required to take action if they are able to. The guidance to the UN GGE Report 2021 affirms this assumption and asserts that also transit states shoulder a due diligence obligation, provided that all other conditions for due diligence obligations are met.[156]

Absent a notification, it is uncertain under which circumstances constructive knowledge can be assumed. Plausibly, a significant increase in bandwidth usage during a DDoS attack or the fact that a state regularly employs certain internet traffic monitoring mechanisms may be indicators for assuming a state's constructive knowledge of an ongoing harmful cyber operation.[157]

4. Required measures

Once a state's knowledge can be assumed, there is so far no clarity on which precise steps the respective state is required to take. The 'appropriate measures' mentioned in Art. 5 lit. b of the ILC Draft Conclusions on the Allocation of Loss are also reiterated in the statement by South Korea which

153 August Reinisch/Markus Beham, 'Mitigating Risks: Inter-State Due Diligence Obligations in Case of Harmful Cyber Incidents and Malicious Cyber Activity – Obligations of the Transit State', *German Yearbook of International Law* 58 (2015) 101–112, at 103.

154 Noting that the group of experts was split Schmitt, 'Tallinn Manual 2.0' 2017 (n. 14), commentary to rule 9, p. 55, para. 3.

155 Republic of Korea, 'Comments' 2020 (n. 30), p. 5; France, Revue stratégique 2018 (n. 117), 86.

156 UN GGE Report 2021, para. 29: 'This norm [para. 13c – the harm prevention rule reference in the UN GGE Report 2015, addition by the author] reflects an expectation that if a State is aware of or is notified in good faith that an internationally wrongful act conducted using ICTs is emanating from or transiting through its territory (…)'; extending the notion of transit state to any state affected by a botnet may risk overstretching the scope of due diligence requirements and may violate rights of individuals Lahmann Unilateral Remedies' 2020 (n. 146), 160; on general conditions for triggering due diligence requirements see above chapter 2.A.I-IV.

157 In more detail on the constructive knowledge standard in cyberspace see chapter 4.D.2.

affirms that it will take 'take all reasonable steps, within [its] territory, to cause these activities to cease, or to mitigate its consequences'.[158] The Netherlands referred to 'shut[ting] down'[159] servers which conduct a cyber attack, Australia to '[reasonable measures to put an end to harmful activities]'[160] and Germany asserted that 'do[ing] nothing' leads to state responsibility.[161] To contribute to better procedures for incident response South Korea suggested to establish a 'universal template for notification and [to] establish the relevant national point of contact'.[162] Already the UN GGE Report 2015 highlighted the benefit of 'procedures for mutual assistance in responding to incidents'[163], similar to the UN GGE Report 2021 which underlined the value of 'common and transparent processes and procedures for requesting assistance'.[164] While states have discretion to discharge the obligation[165] and a duty to stop or mitigate would in any case only be a best efforts obligation[166], it is clear that a blank refusal to cooperate would fall short of the required incident response. It is also clear that the action of CERTs will regularly be crucial for assisting with regard to cyber incidents.[167]

It may be enquired whether a state which lacks the capacity to mitigate an ongoing attack may be under a duty to request assistance from public or

158 Republic of Korea, 'Comments' 2020 (n. 30), p. 5.
159 Netherlands, 'International Law in Cyberspace' 2019 (n. 32), p. 4.
160 Australia, 'Cyber Engagement Strategy' 2017 (n. 149), p. 91.
161 Germany, A/66/152 (n. 141), p. 10.
162 Republic of Korea, 'Comments' 2020 (n. 30), p. 5.
163 UN GGE Report 2015, para. 21d: 'States should consider the following voluntary measures to provide technical and other assistance to build capacity in securing ICTs in countries requiring and requesting assistance (…) (d) Create procedures for mutual assistance in responding to incidents and addressing short-term problems in securing networks, including procedures for expedited assistance.'
164 UN GGE, Report 2021, para 54: 'Common and transparent processes and procedures for requesting assistance from another State and for responding to requests for assistance can facilitate the cooperation described by this norm (…)'; highlighting the need for more opinio iuris Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views ', *The Hague Programe for Cyber Norms – A Policy Brief,* March 2020, p. 12.
165 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 14), commentary to rule 7, p. 44, para. 6.
166 Reflecting the best efforts character of the obligation Canada, Canada's implementation of the 2015 GGE norms, 2019, p. 12; 'When Canada receives a request for assistance from another State whose CI is subject to malicious ICT acts, we respond and do our best to assist that State, and to address any threat emanating from Canadian territory.'
167 On the establishment of CERTs as a due diligence requirement see chapter 4.D.IV.

private actors. International law in some instances stipulates such duties to seek assistance. Art. 11 of the ILC Draft Articles on the Protection of Persons in the Event of Disasters for example requires states to seek assistance if a disaster 'manifestly exceeds its national response capacity'.[168] Also Art. 4 of the ILC Draft Articles on Prevention asserts that seeking assistance 'as necessary' may be required.[169] In the cyber context, the UN GGE Report 2021 referred to the possibility that a state with limited capacity 'may consider seeking assistance from other states or the private sector'[170]. Notably, Canada and Ecuador highlighted this in the UN OEWG as a possibility as well, albeit in hortatory terms.[171] As a duty to require assistance from the private sector or other states would significantly curtail state sovereignty such a duty necessarily needs to be limited to exceptional circumstances. Yet, with regard to the problem of cyber safe havens for the global stability of cyberspace a duty to request assistance, for example with regard to cyber operations that pose a risk for the life and safety of individuals or that have a significant impact on key critical infrastructure of another state, should not be excluded.[172] If such a possibility was excluded from the outset, an affected state may under certain circumstances only be able to resort to measures of self-help against the incapable state, e.g. by invoking necessity under Art. 25 ARSIWA.[173] This would arguably be even more intrusive upon state sovereignty.

168 ILC, Draft articles on the protection of persons in the event of disasters, with commentaries, Yearbook of the International Law Commission, 2016, vol. II, Part Two, art. 11: 'To the extent that a disaster manifestly exceeds its national response capacity, the affected State has the duty to seek assistance from, as appropriate, other States, the United Nations, and other potential assisting actors.'

169 ILC Draft Articles on Prevention 2001 (n. 31), art. 4: 'States concerned shall cooperate in good faith and, as necessary, seek the assistance of one or more competent international organizations', commentary to art. 4, p. 156, para. 6: 'The principle of cooperation means that it is preferable that such requests be made by all States concerned. The fact, however, that all States concerned do not seek necessary assistance does not free individual States from the obligation to seek assistance (…)'.

170 UN GGE Report 2021, para. 30b.

171 UN OEWG Chair's Summary, A/AC.290/2021/CRP.3, 10 March 2021, p. 12 (Canada), p. 18 (Ecuador).

172 Monnheimer, 'Due Diligence ' 2021 (n. 36), 121.

173 Arguing that self-help measures may be justified by necessity, however in very limited circumstances Lahmann, 'Unilateral Remedies' 2020 (n. 146). 204f., 255.

5. Widespread support of a due diligence obligation to take action in cyberspace

Therefore, the duty to take action against imminent and ongoing cyber operations has found widespread support by states and commentators.[174] States are well advised to further specify the precise contours of when assistance obligations are triggered, under which conditions knowledge can be presumed, and which precise measures are to be taken.[175] Operational templates for incident response may significantly contribute to clarifying required standard. A duty to take action in cases of emanating harm can be considered a key procedural due diligence requirement. As was pointed out by *Milanovic/Schmitt:* '[W]hy would any responsible state not take feasible measures to put an end to [harmful] activity'[176]?

III. Duty to notify

A further procedural due diligence requirement may be a duty to notify other states about known risks of harm.

1. Duty to notify in international law and with regard to due diligence

In international law duties to warn in emergency situations exist in numerous treaties, such as with regard to oil pollution[177], nuclear incidents[178], in the law of international watercourses[179], or for the protection of human rights.[180] Also the ILC Draft Articles on Prevention assert a duty to warn in

174 Bannelier/Christakis, 'Prevention Reactions' 2017 (n. 151) 32.
175 Roguski, 'Comparative Analysis' 2020 (n. 164), 12.
176 Schmitt/Milanovic, 'Cyber (Mis)information' 2020 (n. 81), 281.
177 International Convention on Oil Pollution Preparedness, Response and Cooperation, 30 November 1990, 1995 UNTS 78, art. 5 lit.c.
178 Convention on Early Notification of a Nuclear Accident, 26 September 1986, 1439 UNTS 275, art. 5.
179 Convention on the Law of the Non-navigational Uses of International Watercourses of 21 May 1997, 2999 UNTS, art. 28.
180 ILC, 'Draft Articles Disasters' (n. 168), art. 3a: 'For the purposes of the present draft articles: (a) "disaster" means a calamitous event or series of events resulting in widespread loss of life, great human suffering and distress(…)'; art. 9 (2): 'Disaster risk reduction measures include the conduct of risk assessments, the collection and

the case of an emergency.[181] Beyond treaty law international tribunals have asserted a duty to warn about dangers in their territory.

First, in a passage in *Trail Smelter* case the Tribunal already asserted a duty to warn in case an emission reached a certain threshold.[182] It is not clear if the Tribunal based its finding on domestic or international law but the link between warning and harm mitigation already became evident. In the *Corfu Channel* case in which Albania failed to warn the UK of mines in its territorial sea Judge *Alvarez* poignantly asserted in his Separate Opinion:

> '[A] State is bound to give immediate information to countries that are concerned regarding the existence in its territory of dangers, resulting from the action of other States, that have been brought to its knowledge, and which might cause injury to the said countries'[183]

The court's stance in *Corfu Channel* is noteworthy as it makes clear that a duty to warn is based on 'elementary considerations of humanity', hereby indicating that the reasoning is of a general character and not restricted to a specific area of international law.[184] The judgment furthermore makes clear that warning about risks of harm may be required under due diligence for harm prevention. Although the case did not explicitly refer to due diligence this was the undercurrent of the decision.[185] Beyond the Draft Prevention Articles the ILC has also underlined the importance of warning in its Draft Principles on the Allocation of Loss[186], as has the UN Security Council

---

dissemination of risk and past loss information, and the installation and operation of early warning systems'.

181 ILC Draft Articles on Prevention 2001 (n. 31), commentary to art. 17: 'The State of origin shall, without delay and by the most expeditious means, at its disposal, notify the State likely to be affected of an emergency concerning an activity within the scope of the present articles and provide it with all relevant and available information.'

182 *Trail Smelter Case (United States v. Canada)*, Decisions of 16 April 1938 and 11 March 1941, vol. III, UNRIAA, 1905–1982, at 1970.

183 ICJ, *Corfu Channel Case (United Kingdom v. Albania)*, Judgment of 9 April 1949, Separate Opinion of Judge Alvarez, ICJ Reports 1949, p. 39, 45, para. 6; concurring with the judgment, Judgment of 9 April 1949, p. 23.

184 Okowa, 'Procedural Obligations' 1997 (n. 91), 331.

185 Krieger/Peters, 'Structural Change' 2020 (n. 79), 357. The ILC Allocation of Loss principle; makes clear that the duty to warn in itself is also a due diligence obligation, see Allocation of Loss, 2006 (n. 107), commentary to principle 5, p. 167, para. 2.

186 Allocation of Loss, 2006 (n. 107), principle 5a: 'Upon the occurrence of an incident involving a hazardous activity which results or is likely to result in transboundary

with regard to the prevention of terrorist acts.[187] A duty to warn about harmful activities was reiterated by the ICJ in Nicaragua as well.[188] A duty to warn about risks of harm emanating from a state's territory is hence firmly anchored in international law and a recognized procedural sub-duty of due diligence.

2. Duty to notify in cyberspace

In cyberspace, the existence of early warning systems for malicious cyber operations against critical infrastructure was already mentioned in UN General Assembly Res. 58/199 in 2004.[189] Also commentators have underlined its stabilizing value.[190] Yet, so far, states have acknowledged a duty to notify only lukewarmly. A CoE Report of 2010 acknowledged a duty to provide timely notification about threats to the general integrity of the internet.[191] Ecuador acknowledged that informing another state of a harmful activity may be required to discharge due diligence, but did so in notably hortatory terms.[192] Also the Joint Statement of Russia and

damage: (a) the State of origin shall promptly notify all States affected or likely to be affected of the incident and the possible effects of the transboundary damage'.

187 UN, Security Council, Resolution 1373, S/RES/1373, 28 September 2001, para. 2b: 'States shall (…) (b) Take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information.".

188 ICJ, *Military Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment of 27 June 1986, ICJ Reports 1986, p. 14, 103, para. 215.

189 UN General Assembly Resolution A/RES/58/199, 23 December 2003, Annex Elements for protecting critical information infrastructures, para. 1: 'Have emergency warning networks regarding cyber-vulnerabilities, threats and incidents.'

190 Arguing for a duty to notify with regard to cyber espionage Heike Krieger, 'Krieg gegen anonymous', *Archiv des Völkerrechts* 50 (2012), 1–20, at 8.

191 Interim report of the Ad-hoc Advisory Group on Cross-border Internet to the Steering Committee on the Media and New Communication Services incorporating analysis of proposals for international and multi-stakeholder co-operation on cross-border Internet, H/Inf (Council of Europe 2010), p. 21, para. 91f.: 'states should take all reasonable measures to provide prior and timely notification and relevant information to states that may be potentially affected [by disruption to or interferences with the stability and resilience of Internet resources, addition by the author].'

192 Ecuador preliminary comments to the Chair's "Initial pre-draft" of the Report of the United Nations Open Ended Working Group on developments in the field of information and telecommunications in the context of international security (UN

China[193] which refers to 'information-sharing' seems at this point as a mere normative aspiration. While India acknowledged the relevance of early warning for cyber threats against critical infrastructure[194] it fell short of further endorsing a duty to warn but rather allocated warning mechanism as a CBM. Early warning mechanisms were also mentioned as a CBM by China.[195] A general duty to warn about risks of cyber harm is notably absent throughout statements of states and in the work of the UN GGE and the UN OEWG. Overall, states have hence avoided to commit to an obligation or responsibility to notify. Yet, it is also noteworthy that states have not explicitly rejected a duty to notify.

3. Reluctance of states to commit to a duty to notify in cyberspace

A reason for the reluctance of states may inter alia be that the disclosure of information may reveal a state's intelligence capacities.[196] Art. 14 of the ILC Draft Prevention Articles acknowledges that national security interests may be an interest which limits a state's duty to notify.[197] The reluctance

OEWG), p. 2: 'State identifies malicious cyber activity emanating from another State's region or cyberinfrastructure, a first step could be notifying that State.'

193 The Joint Statement Between the Presidents of the People's Republic of China and the Russian Federation on Cooperation in Information Space Development, 26 June 2016, para. 7: 'Advance cooperation in information security emergency response and information sharing of information security threat, and enhance cross-border information security threat management'.

194 India, Latest Edits to Zero Draft, 2021, p. 14, para. 88: 'Information sharing and coordination at the national, regional and international levels can make capacity-building activities more effective, strategic and aligned to national priorities.

195 Statement Yao, 'Critical Infrastructure' 2020 (n. 8): 'States should (…) explore the possibilities to establish relevant risk early warning and information sharing mechanism (…)'.

196 Oren Gross, 'Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents', *Cornell International Law Journal* 48 (2015), 481–511, at 504.

197 ILC Draft Articles on Prevention 2001 (n. 31), art. 14: 'National security and industrial secrets Data and information vital to the national security of the State of origin or to the protection of industrial secrets or concerning intellectual property may be withheld, but the State of origin shall cooperate in good faith with the State likely to be affected in providing as much information as possible under the circumstances.' In the context of the ILC draft prevention articles this caveat applies to information to the public (in Art. 13) but the rationale similarly applies to notification to other states.

of states may furthermore be due to the lack of certainty under which circumstances a duty to inform may be triggered. It is not fully clear to whom a duty to warn would be owed. On the one hand, it is relatively clear that it would cover states which are affected, or potentially affected by a harmful operation.[198] On the other hand, a duty to warn may extend to a duty to warn the public about dangers. The UN OEWG notably mentions the notification of users about ICT vulnerabilities as a CBM.[199] Moreover, para. 13 lit. j of the UN GGE Report 2015 is primarily addressed at disclosure of vulnerabilities to the public.[200] Also the 2010 CoE Advisory Report highlights that information sharing on ICT vulnerabilities between private actors is an important aspect for ensuring cyber resilience of critical infrastructure.[201] Informing the public likely affected by harmful activities is foreseen in Art. 13 of the ILC Draft Prevention Articles as well.[202]

The repeated emphasis on information to the public evokes the question whether such a duty could be conceived as a requirement under the harm prevention rule or whether it should rather be conceived as a protective duty under human rights law. Statements of states so far do not clarify the legal basis for informing the public and individuals. The more plausible claim is that a duty to notify and inform the public is a due diligence requirement only under the duty to protect in international human rights law as it is acknowledged that notification with regard to grave risks can be required under international human rights law.[203] By contrast, the harm

198 Ecuador, 'Preliminary comments' 2020 (n. 192), ILC Draft Articles on Prevention 2001 (n. 31), art. 8 (1).

199 UN OEWG, zero draft, para. 50; revised draft, para. 42, initial draft para. 38.

200 UN GGE Report 2015, para. 13j: 'States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.' See in more depth on disclosure of vulnerabilities in chapter 4.C.V.3. For an alternative reading that it may be also require reporting to other states in the light of the due diligence rationale see Nicholas Tsagourias, 'Recommendation 13j', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 241–264, p. 261, para. 36.

201 Ad-hoc Advisory Group on Cross-border Internet, 'Interim Report' 2010 (n. 201), p.21, para. 91.

202 ILC Draft Articles on Prevention 2001 (n. 31), art. 14.

203 ECtHR, *Case of Budayeva and Others v. Russia*, Judgment of 20 March 2008, Application Nos 15339/02 et al., para. 162, 176; Baade, 'The Duty to Protect' 2020 (n. 64), 103.

prevention rule, as an inter-state obligation, is owed primarily to affected states, but not to individuals or the general public. Nevertheless, the mention of information to the public in the part of the UN GGE Report on norms of responsible state behaviour at least suggests that it can also be in the interests of other states that the public – which may also include other states – is informed.[204]

States have so far not specified the procedure and timing for diligence duties to warn in cyberspace. Under customary international law it is clear that the notification has to follow immediately upon acquiring knowledge[205], in the case of disasters 'without delay and by the most expeditious means'.[206] Furthermore, it should include 'all relevant and available information'.[207] With regard to contact points the now-repealed EU Directive on the security of network and information system (NIS Directive) exemplarily asserted that it should go through trusted channels.[208] It may moreover be considered good practice to include information of the scope and gravity of the risk of harm.[209]

4. Nascent emergence of a due diligence obligation to notify in cyberspace

There are strong reasons to assume a duty to notify other states about impending attacks exists.[210] While general rules on due diligence for harm prevention strongly support such a duty the reluctance of states and their tentative relegation of notification to the level of capacity building or CBMs so far weakens the normative pull of such a diligence requirement in cyber-

204 See Tsagourias, 'Recommendation 13j' 2017 (n. 200), para. 36.

205 ILC Allocation of Loss, 2006 (n. 107), commentary to principle 5, p. 167, para. 2: 'The notification obligation has to be performed as soon as it is practicable'. Okowa, 'Procedural Obligations' 1997 (n. 91), 295.

206 ILC Draft Articles on Prevention 2001 (n. 31), art. 17.

207 Ibid.

208 EU, Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS 1 directive), para. 59.

209 As e.g. foreseen in ILC Draft Articles on Prevention 2001 (n. 31) art. 13.

210 See also Gross, 'Cyber Responsibility' 2015 (n. 196), 503; Adamson, 'Recommendation 13c' 2017 (n. 29), p. 72, 73, para. 35*:* 'Exchange of information is an essential facilitating element of effectively exercising due diligence. It covers inter alia the exchange of information about risks of significant transboundary harm with the potentially affected parties, potential threats in general, information about vulnerabilities, as well as sharing information for the investigation and prosecution purposes.'

space. A due diligence obligation to notify about risks of cyber harm is hence only nascently emerging. Similar to other potential due diligence requirements the lack of a sufficiently precise legal content seems to inhibit states to commit to a duty to notify, potentially due to concerns to expose intelligence capabilities. States are well advised to be more forthcoming with regard to their opinio iuris. Best practice templates may provide a stabilizing next step towards the evolution of an international legal standard.

IV. Duty to cooperate on the prosecution of cybercrime

A study by the European Commission in 2018 found that more than half of cybercrime investigations involve a transnational element.[211] Accessing and securing relevant evidence stored abroad is however difficult due to enforcement jurisdiction limits. In principle, it is the exclusive right of the territorial state to access data stored on its territory for law enforcement purposes. As a consequence, international cooperation for securing evidence and for apprehending perpetrators is necessary.[212] While efficient cooperation presupposes institutional safeguards[213] the main emphasis of cooperation with regard to prosecution of cybercrime lies on procedures for coordinated action. It is hence discussed here as a potential *procedural* due diligence obligation.

211 European Commission Staff Working Document, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceeding, 17 April 2018, SWD/2018/118 final; see also Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation', *Monash University Law Review* 40 (2015), 698–736, at 700.

212 Theodore Christakis/Fabien Terpan, 'EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options', *International Data Privacy Law* 11 (2021), 81–106; Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations Under International Law* (Intersentia 2014), 30.

213 See below chapter 4.D.I.on cybercrime legislation as a due diligence requirement.

1. Prohibition of extraterritorial law enforcement as a challenge for cybercrime prosecution

The collection of evidence on servers located abroad without the consent of the territorial state regularly violates the exclusive right of territorial law enforcement of the territorial state.[214] The only mechanism by which the consent of the territorial state can be sidelined are direct access procedures which enable law enforcement agencies to directly request data from private service providers. Yet, such procedures, as e.g. foreseen in Art. 32 lit. b of the Budapest Convention on Cybercrime[215], are so far limited to like-minded countries. Due to the stance of several countries on 'sovereign control' over national cyberspace and the challenges of securing due process safeguards regarding direct access this is unlikely to change.[216] Current attempts to legalize direct access to private service providers for obtaining evidence, circumventing the mutual legal assistance process, have also been criticized as a potential 'race to the bottom' for human rights safeguards.[217]

214 UN ODC, Comprehensive Study on Cybercrime, February 2013, p. 184; Michael Schmitt/Liis Vihul, 'Respect for Sovereignty in Cyberspace', *Texas Law Review* 95 (2017), 1639–1670, at 1660; on the exclusive right to exercise state power Przemysław Roguski, 'Violations of Territorial Sovereignty in Cyberspace – an Intrusion-Based Approach', in Dennis Broeders/Bibi van den Berg (eds.), *Governing Cyberspace: Behaviour, Power and Diplomacy* (London: Rowman & Littlefield 2020), 65–84, at 74, inter alia referring to PCIJ, *The Case of the S.S. Lotus (France v. Turkey)*, Judgment of 7 September 1927, Series A, No. 10, p. 4 at 18, 19: '[F]ailing the existence of a permissive rule to the contrary [a State] may not exercise its power in any form in the territory of another State'.

215 Council of Europe Convention on Cybercrime, 23 November 2001, ETS 2001, No. 185, art. 32 lit.b: 'A Party may, without the authorisation of another Party (…) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.'

216 Russia e.g. fiercely opposes Art. 32 lit. b of the Budapest Convention as it views it as a violation of state sovereignty, see EDRI, 'Transborder data access: Strong critics on plans to extend CoE Cybercrime Treaty', 5 June 2013, available at: https://edri.org/our-work/edrigramnumber11-11transborder-data-access-cybercrime-treaty/.

217 EDRI, New Protocol on cybercrime: a recipe for human rights abuse?, 25 July 2018, available at: https://edri.org/our-work/new-protocol-on-cybercrime-a-recipe-for-human-rights-abuse/; the EU Draft Production Order hence foresees the non-execution of Production Orders if the private service provider considers that compliance with a production order would violate the law of a third state, e.g. fundamental rights stipulated in the law of the third's state, see EU, Proposal for a Regulation of the European Parliament and of the Council on European

Therefore, inter-state cooperation, in particular with regard to the securing and accessing of digital evidence, is key to efficient cybercrime prosecution.[218]

2. Cooperation in legal instruments on cybercrime: Discussions on the UN level

On the UN level, the necessity of cooperation with regard to cybercrime is repeatedly stressed in resolutions of the UN General Assembly[219] It has also featured prominently in the negotiations of an international convention on cybercrime.[220] States have not directly linked cooperation on cybercrime to due diligence but an integrative reading of the norms of responsible state behaviour[221], including the general cooperative aspiration in para. 13 lit. a[222], suggests that cooperation for cybercrime can be conceived as part of the diligence required under para. 13 lit. c of the UN GGE Report 2015. Yet, the UN GGE assertion regarding cooperation on cybercrime prosecution is poignantly hortatory. Para. 13 lit. d of the UN GGE Report of 2015 broadly stipulates that:

> 'States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may

Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final – 2018/0108 (COD), 17 April 2018, art. 15, 16.

218 See also UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 183f.

219 See already UN General Assembly Resolution A/RES/58/199, 23 December 2003, Annex, para. 10: 'Engage in international cooperation, when appropriate, to secure critical information infrastructures, including by (…) coordinating investigations of attacks on such infrastructures in accordance with domestic laws.'

220 See UN GA, Ad Hoc Committee to Elaborate a Comprehnsive International Convention on Countering the Use of Information and Communictions Technologies for Criminal Purposes, A/AC.291/22, 29 May 2023, art. 35 (1): 'States Parties shall cooperate with each other in accordance with the provisions of this Convention, as well as other applicable international instruments on international cooperation in criminal matters (...).'

221 Homburger, 'Recommendation 13 a' 2017 (n. 99), p. 10, para. 2; see also above chapter 4.B.III.

222 See above chapter 4.C.I.

> need to consider whether new measures need to be developed in this respect'.[223]

In slightly more assertive language the UN GGE 2013 notably stated that:

> 'States should intensify cooperation against criminal or terrorist use of ICTs, harmonize legal approaches as appropriate and strengthen practical collaboration between respective law enforcement and prosecutorial agencies'.[224]

The poignantly hortatory language of the UN GGE Reports hence entails little normative substance and is more akin to an optimization aspiration than to a firm legal commitment. Also the assertion that states may resort to voluntary agreements on cybercrime cooperation as a non-binding CBM underlines that the UN GGE Reports largely relegate cybercrime cooperation to the level of non-binding norms:

> 'States should consider additional confidence-building measures that would strengthen cooperation on a bilateral, subregional, regional and multilateral basis. These could include voluntary agreements by States to: (…) (e) Cooperate, in a manner consistent with national and international law, with requests from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.'[225]

3. Cooperation requirements in cybercrime treaties

A reason for the reluctance of states in the UN GGE Report inter alia may be that states want to avoid contradictions or frictions with cooperation requirements under regional cybercrime treaties. Several binding cybercrime

223 UN GGE Report 2015, para. 13 lit. d; on the implementation of para. 13 lit.d see UN GGE Report 2021, para. 32: 'Observance of this norm implies the existence of national policies, legislation, structures and mechanisms that facilitate cooperation across borders on technical, law enforcement, legal and diplomatic matters relevant to addressing criminal and terrorist use of ICTs.' Para. 33: '(…) States are also encouraged to develop appropriate protocols and procedures for collecting, handling and storing online evidence relevant to criminal and terrorist use of ICTs and provide assistance in investigations in a timely manner, ensuring that such actions are taken in accordance with a State's obligations under international law.'

224 UN GGE Report 2013, para. 22.

225 UN GGE Report 2015, para. 17 lit.d.

treaties stipulate duties to cooperate on cybercrime prosecution.[226] Art. 23 of the Budapest Conventions e.g. stipulates that states shall cooperate to the widest extent possible in criminal matters and with regard to mutual legal assistance requests.[227] Similarly, Art. 34 of the Arab League Convention stipulates cooperation requirements and procedures regarding mutual legal assistance.[228] Furthermore, several non-binding MoU entail agreements to cooperate in cybercrime prosecution. For example, the MoU between China and the US of 2015 asserts that both states '[agree to cooperate with regard to requests to investigate cybercrimes]'.[229] Further similar MoUs on cooperation exist, frequently reiterating the intent to cooperate on cybercrime without further specification.[230]

Overall, hence, a wide net of binding and non-binding cooperation norms regarding cooperation on prosecution of cybercrime exists, underlining that cooperation for cybercrime is regularly a normative expectation in international law. Regarding the complexity of the wide net of binding and non-binding cooperation norms it however remains the question

226 On cybercrime legislation as a due diligence requirement see below chapter 4.D.I.

227 Convention on Cybercrime 2001 (n. 215), art. 23: 'The Parties shall co-operate with each other (…) to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.' See also ibid., art. 25: 'The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence'.

228 Arab League, Convention on Combating Information Technology Offences, 21 December 2010, art. 34 (6): 'The State Party from which assistance is requested shall commit itself to inform the requesting State Party of the result of the implementation of the request. If the request is refused or postponed, the reasons of such refusal or postponement shall be given. The State Party from which assistance is requested shall inform the requesting State Party of the reasons that prevent the complete fulfillment of the request or the reasons for its considerable postponement.'

229 However, under the precondition that cooperation requirements comply with domestic law, see U.S.-China Cyber Agreement, 16 October 2015: 'The United States and China agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities. Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory.'

230 E.g. ASEAN-EU, 'Statement' 2019 (n. 126), para. 11; Memorandum of Understanding between the Government of the Republic of Indonesia and the Government of Australia on Cyber Cooperation, 31 August 2018, para. 2 (4).

whether an objective minimum standard as a bottom line and least common denominator can be deduced as a binding due diligence requirement.

4. Tracing international legal standards for cybercrime cooperation

There are two main tracks of cooperation on cybercrime prosecution: Formal cooperation, mainly in the form of mutual legal assistance requests, and informal cooperation, through direct law enforcement cooperation, agency-agency cooperation or cooperation between liaison officers.[231]

4.1 Formal cooperation: Mutual legal assistance

Formal cybercrime cooperation is primarily channelled via mutual legal assistance. Mutual legal assistance is no general obligation under international law but is stipulated by a variety of mutual legal assistance treaties, mostly on a bilateral and in some cases regional level. Such regional and bilateral mutual legal assistance treaties in criminal matters often exist alongside treaties on administrative mutual legal assistance, and treaties on civil and commercial legal assistance.[232] The function of mutual legal assistance is to make cooperation in criminal prosecution more timely and more reliable and to facilitate direct contact between judicial authorities.[233] The treaties for example address securing and obtaining evidence, or the apprehension and extradition of persons.[234] Due to the increasing transnational dimension of various criminal activities, for example human trafficking, the importance of mutual legal assistance in international relations has been growing.

With regard to cybercrime the Budapest Convention and the Arab League Convention stipulate specific rules for mutual legal assistance in inves-

231 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 187.

232 Dieter Martiny, 'Mutual Legal Assistance in Civil and Commercial Matters', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2009), para. 1f.

233 Time René Salomon, 'Mutual Legal Assistance in Criminal Matters', in Rüdiger Wolfrum (ed.), *Max Planck Encyclopedia of Public International Law* (Oxford: Oxford University Press 2013), para. 11.

234 See Convention on Cybercrime 2001 (n. 215), art. 24, Arab Convention (n. 228), art. 31; UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 199.

tigations[235], but also general mutual legal assistance treaties may apply to cybercrime investigations.[236]

4.2 Principles and limits of mutual legal assistance

Important principles of mutual legal assistance are the principle of reciprocity, dual criminality and mutual recognition.[237] A state will only take law enforcement measures after a mutual legal assistance request if it considers the conduct in question criminal as well. As states homogeneously criminalize core cyber offences against the confidentiality, integrity and availability of ICT[238] the issue of dual criminality is not insurmountable regarding cyber harm.[239] Yet, mutual legal assistance agreements entail multiple reasons which allow a state to reject a request. A state may for example refuse requests due to incompatibility with domestic law, e.g. with constitutional rights. In the cyber context, a state can for instance refuse a request due to its incompatibility with privacy or data protection rules. In this regard, the problem that states' standards and safeguards for protecting individual rights diverge becomes acute.[240] Furthermore, states may refuse requests due to national security concerns or essential security interests of a state, as can for example be seen in the ICJ case in *Djbouti vs. France*.[241] Also the Budapest Convention entails a provision recognizing that 'it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests'.[242] Ultimately, mutual legal assistance depends to a significant extent on the political will

235 See Convention on Cybercrime 2001 (n. 215), art. 24, Arab Convention (n. 228), arts. 34, 39, 41, 42.

236 Clough, 'Challenges of Harmonisation' 2015 (n. 211), 731.

237 On the importance of the dual criminality rule see UN ODC, 'Comprehensive Study' 2013 (n. 214), p.60.

238 See on converging standards regarding key cybercrime offences in more detail below chapter 4.D.I.4.2. However, with regard to content crimes, this is likely to be different.

239 Under the Budapest Convention states are encouraged to apply a flexible approach when applying dual criminality, see Explanatory Report to the Convention on Cybercrime, 23 November 2001, para. 259.

240 See on diverging safeguards and standards of in criminal procedural law, e.g. regarding time limits, judicial review, or limited list of offences chapter 4.D.I.5.2.

241 ICJ, *Case Concerning Certain Questions of Mutual Assistance in Criminal Matters (Djibouti/France),* Judgment of 4 June 2008, ICJ Reports 2008, 177, para. 135.

242 Convention on Cybercrime 2001 (n. 215), art. 27.

of a requested state and mutual trust between state parties. Such mutual trust may be difficult to achieve in cyberspace.[243] The statement of Russian president Putin with regard to request extradition of cybercriminals stands emblematically for the limits of mutual legal assistance when political will and mutual trust are missing:

> 'Russia will naturally [extradite] but only if the other side, in this case the United States, agrees to the same and will also extradite corresponding criminals to the Russian Federation.'[244]

The variety of recognized broad reasons for rejecting requests puts into question whether a minimum standard of cooperation can be assumed. One may however enquire whether states at least need to give reasons for refusing a request. In the ICJ case *Djibouti vs France* France was for example held accountable for failing to give reasons for its refusal of a mutual legal assistance request.[245] The duty to give reasons for a refusal to cooperate in criminal proceedings has also been acknowledged in international human rights law by the ECtHR.[246] Also the principle of good faith which is stipulated by Art. 4 of the ILC Draft Prevention Articles weighs in favour of assuming a duty to at least give reasons for refusing a cooperation request.[247]

Assuming such a duty would heighten the argumentative burden of uncooperative states. A duty to give reasons for rejecting cooperation may also incentivize states to establish responsible entities for international requests.[248] In particular, with regard to highly harmful cyber operations, refusals to cooperate may be hard to justify. Thus, it can be assumed that responding to and giving reasons for refusals of an assistance request are a binding minimum requirement.

---

243 De Busser, 'Recommendation 13d' 2017 (n. 119), para. 32.

244 Olga Pavlova, 'Putin says Russia prepared to extradite cyber criminals to US on reciprocal basis', *CNN,* 13 June 2021, available at: https://edition.cnn.com/2021/06/13/europe/putin-russia-cyber-criminals-intl/index.html.

245 ICJ, 'Mutual Legal Assistance in Criminal Matters' (n. 241), para. 156.

246 ECtHR, *Case of Güzelyurtlu and Others v. Cyprus and Turkey*, Grand Chamber Judgment of 29 January 2019, Application no. 36925/07, para, 266.

247 ILC Draft Articles on Prevention 2001 (n. 31), art. 4: 'States concerned shall cooperate in good faith (…)'; In the *Djibouti/France* case Djibouti argued that the lack of reasons provided by France regarding its refusal to cooperate violated good faith, see ICJ, 'Mutual Legal Assistance in Criminal Matters' (n. 241), para. 135.

248 On the importance of establishing points of contact for cybercrime prosecution see below chapter 4.D.IV.

4.3 Informal cooperation

Mutual legal assistance is often perceived as too slow and ineffective.[249] As a consequence, states have partially resorted to informal procedures, such as agency-agency cooperation, or direct contact between law-enforcement authorities, at times facilitated by an international agency, such as INTERPOL.[250] Informal cooperation can facilitate and accelerate formal cooperation[251] but it is so far under-utilized. There are several 'success' stories of informal cooperation. Yet, most states do not have a clearly prescribed set of rules for informal cooperation.[252] Informal cooperation hence lacks a sufficient level of coherency to inform a minimum or best practice due diligence standard. Furthermore, informal cooperation bears the risk of watering down procedural safeguards, in particular due process rights.

5. The challenge of assessing cybercrime cooperation standards beyond a minimum standard

Due to diverging standards in international practice and a complex web of international standards, a uniform due diligence standard of cooperation on cybercrime prosecution cannot be presumed. The UN GGE Reports and the wide net of formal and non-binding norms on cooperation regarding cybercrime however regularly create the normative presumption that states cooperate in good faith on cybercrime prosecution. As a bottom line states are required to give reasons for rejecting formal cooperation requests. To avoid the risk that cooperation is only fragmentary or limited to regional hubs, states are well advised to improve mutual legal assistance agreements

249 T-CY Cybercrime Convention Committee, T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime T-CY(2013)17rev (Provisional), Strasbourg, France 3 December 2014 T-CY assessment report: p. 123: 'Response times to requests of six to 24 months appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the positive obligation of governments to protect society', See also Anna Maria Osula, 'Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data', *Masaryk University Journal of Law and Technology* 9 (2015), 43–64, at 51.

250 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 209; see also Berkes, 'Human Rights in Cyberspace' 2019 (n. 62), 226.

251 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 209.

252 Ibid., p. 210.

and procedures. The Second Additional Protocol to the Budapest Convention may contribute to this aim.[253] Focusing on the improvement of such formalized procedures via specialized legal rules as *lex specialis* seems eventually more promising than resorting to an open-ended and largely undefined due diligence duty of cybercrime cooperation. In this regard the reluctance of the UN GGE Reports regarding general assertions on cybercrime cooperation requirements may be well reasoned.

V. Risk mitigation measures regarding ICT vulnerabilities

Vulnerabilities are a persistent problem for the security of ICT. Vulnerabilities are weaknesses or errors in the code, design or internal controls that enable the compromising of the CIA of ICT.[254] A vulnerability creates an entry point or an 'attack surface' for potential attackers if they have a tool or a technique to exploit the error.[255] The cross-cutting relevance of ICT vulnerabilities and its link to the integrity of the ICT supply chain[256] raises the question whether the obligation to exercise due diligence for harm prevention requires risk mitigation measures regarding ICT vulnerabilities. ICT vulnerability risk mitigation bundles both negative and positive obligations and with regard to the latter sits at the interface of procedural and institutional due diligence measures. It is discussed here in the context of procedural due diligence measures due to the importance of procedural rules for vulnerability disclosure processes, as well as due to links to other procedural due diligence measures, such as duties to notify or to assist.

253 Council of Europe, Second Additional Protocol **2021 (n.** 145**).** On the necessity of such a protocol, e.g. with regard to more effective procedures and more transparency see Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 March 2019, the UNODC/CCPCJ/EG.4/2019/2, 12 April 2019, paras. 16, 17.

254 In this vein National Institute of Standards and Technology, Glossary, vulnerability.

255 See UN GGE Report 2021, para. 11: 'New and emerging technologies are expanding development opportunities. Yet, their ever-evolving properties and characteristics also expand the attack surface, creating new vectors and vulnerabilities that can be exploited for malicious ICT activity.'

256 UN GGE 2015, para. 13i.

1. Definition of ICT vulnerabilities

The European Union Agency for Cybersecurity (ENISA) defines a vulnerability as

> '[t]he existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event (…) compromising the security of the computer system, network, application, or protocol involved'.[257]

Due to the complexity of programming and designing IT software and IT hardware, as well as time pressure in a competitive market[258], ICT products used by governmental agencies, critical infrastructures and private users inevitably have 'vulnerabilities'.[259] They are embedded in the design of ICT. The more vulnerabilities in IT products exist, the more surface attackers have to attack. As a consequence, wide-spread vulnerabilities risk to undermine the confidence in the global internet[260] and to adversely affect the global culture of cybersecurity. Reduction of vulnerabilities in ICT is hence a central prerequisite for a more resilient cyberspace.[261]

257 ENISA, Glossary, available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary.

258 Thomas Holt, 'What are software vulnerabilities, and why are there so many of them?', *The Conversation*, 23 May 2017, available at: https://theconversation.com/what-are-software-vulnerabilities-and-why-are-there-so-many-of-them-77930.

259 Klaus Lenssen, '…on the Ground: An Industry Perspective', in Ingolf Pernice/Jörg Pohle (eds.), *Privacy and Cyber Security on the Books and on the Ground* (Alexander von Humboldt Institute for Internet and Society 2018), 107–110, 110: 'We must acknowledge and (frustratingly) accept that software, hardware, and services vulnerabilities exist today and will continue to be discovered, no matter how hard we all work to avoid them. With millions of lines of code plus thousands of configuration options, and the ability of a single wrong keystroke to result in a bug that is not detected, complexity is quite possibly the single biggest contributing factor'; see also Lahmann Unilateral Remedies' 2020 (n. 146), 17.

260 Myriam Dunn Cavelty/Jacqueline Eggenschwiler, 'Behavioral Norms in Cyberspace', *The Security Times,* February 2019, p. 35; Lenssen, 'Industry Perspective' 2018 (n. 259), 109.

261 One of the central aims of the EU Cybersecurity Act is the identification of ICT vulnerabilities, see EU Regulation 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act), e.g. Rc. 30, art. 51d, g, j.

2. Exploitation of ICT vulnerabilities by intelligence and law enforcement

From the outset, the issue of ICT vulnerabilities is complicated by the fact that vulnerabilities, also termed 'zero-day exploits'[262], are not only exploited by cyber criminals but also exploited by law enforcement and intelligence services, for example to gather information in investigations or to potentially manipulate the operation of an IT system or network for law enforcement purposes. Hence, states often have an interest in retaining vulnerabilities they have found or bought.[263] The development, sale and distribution of hacking tools is a prolific business. The so-called *Pegasus* disclosures have revealed the widespread sale of the *Pegasus* spyware from the Israeli IT security firm NSO to various governments which in many cases subsequently targeted numerous journalists, human rights activists and politicians.[264] As most such transactions remain clandestine it is not possible to properly assess the number of sales of cyber 'weapons' to governments but disclosures of hackers trading with governments indicate that the number is significant.[265] Hence, it can be assumed that the question of vulnerabilities disclosure is a sensitive matter for the vast majority of states.

Purchasing and retaining a vulnerability is risky. Vulnerabilities may be discovered simultaneously by other malicious actors: According to security researchers between 10–20 % of vulnerabilities get discovered parallelly.[266] Furthermore, retained vulnerabilities may themselves be compromised, leaked or stolen. Before the *WannaCry* attack in 2017 the NSA for example stockpiled a vulnerability in a Microsoft software over years. The vulnerability was subsequently leaked to the group *Shadow Brokers*. After discovering the leak, the NSA disclosed the vulnerability to Microsoft which

262 Kellen Browning, 'Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack', *New York Times,* 2 July 2021, available at:https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html : 'a previously unknown vulnerability in its systems — known as a "zero day" (…) when such vulnerabilities are discovered, software makers have zero days to fix it'.

263 Thomas Wischmeyer, *Informationssicherheit* (Tübingen: Mohr Siebeck 2023), 282.

264 'Revealed: leak uncovers global abuse of cyber-surveillance weapon', *Guardian*, 18 July 2021, available at: https://www.theguardian.com/news/series/pegasus-project.

265 Eleonora Viganò/Michele Loi/Emad Yaghmaei, 'Cybersecurity of Critical Infrastructure', in Markus Christen Bert Gordijn Michele Loi (eds.) *The Ethics of Cybersecurity* (Berlin: Springer Natur 2020), 157–178, at 173, 174.

266 Bruce Schneier, 'Simultaneous Discovery of Vulnerabilities', *Schneier on Security*, 15 February 2016, available at: https://www.schneier.com/blog/archives/2016/02/simultaneous_di.html.

immediately issued a patch in March 2017. Yet, in May 2017 many users had not yet installed the patch and were hence vulnerable to the exploitation of the leaked vulnerability. The ensuing *WannaCry* attack caused massive economic damage and disruptions worldwide. Even some hospitals were partially shut down[267], exemplarily highlighting the risks of retaining vulnerabilities. It raises the question if and under which circumstances due diligence requires states to disclose ICT vulnerabilities they are aware of.

3. Vulnerability disclosure as a due diligence requirement

It has been argued that vulnerability disclosure falls outside of the realm of due diligence from the outset because in case of non-disclosure of a vulnerability by a state it cannot be said that the harmful cyber operation was emanating from that state's territory.[268] However, knowledge of a vulnerability will usually be gained by a state on its territory or under its control. Even if the acquisition of knowledge is not tantamount to control over the harmful actor who is exploiting the vulnerability and may operate on the territory of another state, a state is at least in the position to influence whether a vulnerability can be exploited by this third actor. Hence, it seems justified to assume due diligence-based accountability due to the knowledge-based capacity to influence the harmful act or its effects.[269] Grasping the issue of vulnerabilities disclosure under the due diligence rationale should therefore not be discarded from the outset. The issue of vulnerability disclosure is addressed in para. 13 lit. j of the UN GGE Report 2015 which asserts that:

> 'States should encourage responsible reporting of ICT vulnerabilities and share information on available remedies to such vulnerabilities to limit and possible eliminate potential threats to ICTs and ICT-dependent infrastructure'.

The text of para. 13 lit. j hence concerns two different aspects regarding vulnerabilities: On the one hand, the encouragement of the reporting of a vulnerability and on the other hand, the sharing of information on

267 Russell Brandom, 'UK Hospitals Hit with Massive Ransomware Attack', *The Verge,* 12 May 2017, available at: https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin.

268 Delerue, 'Cyber Operations' 2020 (n. 47), 373.

269 On capacity to influence as the underlying rationale of due diligence-based accountability chapter 2.A.III.

remedies. The text of the norm does not directly address vulnerability disclosure between states.

3.1 Reporting of ICT vulnerabilities

Regarding the regulation of responsible reporting, the text indicates that para. 13 lit. j is primarily conceived within the territory of a state and concerns reporting of discovered vulnerabilities by private actors to vendors. This corresponds to the classical understanding of vulnerability disclosure which circumscribes the process in which the finder informs the vendor (and not other states) of a vulnerability.[270] Para. 13 lit. j stipulates that states 'should encourage responsible reporting' – a normative aim that is also highlighted by the Paris Call of 2018.[271] *Adamson* has referred to the adoption of appropriate legislation as a potential measure.[272] More broadly, Canada has hinted at establishing 'national structures' to encourage reporting[273], similar to the UN GGE Report 2021 which argued for 'impartial legal frameworks, policies and programmes to guide decision-making on the handling of ICT vulnerabilities and curb their commercial distribution'.[274] To encourage reporting of vulnerabilities it is important to provide more legal certainty to 'white-hat' security researchers that they will not be subjected to investigation and prosecution following disclosure of a found vulnerability – an issue which the EU, as well as the UN GGE Report, has highlighted.[275] Too often, benevolent hackers who follow procedures to test the security of ICT products are subject to criminal investigations

270 See the definition under ISO/IEC 29147: 'Vulnerability disclosure is a process through which vendors and vulnerability finders may work cooperatively in finding solutions that reduce the risks associated with a vulnerability.'

271 Paris Call for Trust and Security in Cyberspace, 12 November 2018, p. 2: 'We recognize all actors can support a peaceful cyberspace by encouraging the responsible and coordinated disclosure of vulnerabilities.'

272 Adamson, 'Recommendation 13c' 2017 (n. 29), p. 74, para. 39.

273 Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, UN General Assembly A/75/816, 18 March 2021, Annex to the Chairs summary, Canada, p. 15.

274 UN GGE Report 2021, para. 62.

275 UN GGE Report 2021, para. 62: 'States could also consider putting in place legal protections for researchers and penetration testers.'; EU, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, (NIS 2 Directive),

after disclosing an identified ICT vulnerability. As the precise legislative measures for protecting security researchers are not further specified by states and as the UN GGE Report 2021 only hortatorily refers to the option to consider such measures[276], so far, putting such protections in place can however only be considered best practice.

The degree as to which a state decides to encourage reporting domestically affects the legally protected interests of other states only indirectly. This raises the question to what extent encouragement of reporting can be conceived as a best practice standard under the harm prevention rule.

Some states and commentators view the reporting of vulnerabilities as an obligation on the inter-state level. The text of para. 13 lit. j UN GGE Report 2015 does not indicate this but *Tsagourias* has directly deduced a duty to warn other states about vulnerabilities via a systematic reading of para. 13 lit. j in the light of the due diligence rationale expressed by para. 13 lit. c.[277] States' statements support the reading that international law vulnerability disclosure also applies between states. China, for example, considers reporting of vulnerabilities between states a CBM.[278] Canada referred to cooperation between national CERTs and hence to inter-state cooperation mechanisms to implement para. 13 lit. j of the UN GGE Report.[279] Also the UN GGE presupposes that vulnerability disclosure occurs between countries and national CERTs.[280] Due to the interest of every single state to acquire knowledge about ICT vulnerabilities such a conception of vulnerability disclosure as an inter-state obligation seems reasonable.

Rc. 60: '(…) Member States should aim to address (…) the challenges faced by vulnerability researchers, including their potential exposure to criminal liability(…).'

276 UN GGE Report 2021, para. 62.

277 Tsagourias, 'Recommendation 13j' 2017 (n. 200), para. 36: 'It can thus be contended that, to the extent that a general duty to inform, notify or warn exists in international law, it translates into a duty to inform other states of vulnerabilities that may cause damage to their infrastructure.'

278 China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 2020, p. 7, at V.

279 Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, UN General Assembly A/75/816, 18 March 2021, Annex to the Chairs summary, Canada, p. 11.

280 UN GGE Report 2021, para. 61: 'A coordinated vulnerability disclosure process can minimize the harm to society posed by vulnerable products and systematize the reporting of ICT vulnerabilities and requests for assistance between countries and emergency response teams'.

There are hence strong reasons to assume that the normative expectations to disclose vulnerabilities in principle also apply between states under the harm prevention rule. However, as China's categorization of vulnerability as a mere CBM indicates, a duty to warn about ICT vulnerabilities can, so far, only be considered an emergent norm, but not a binding due diligence requirement.

There is furthermore not yet an approximate standard under which conditions vulnerabilities need to be disclosed. States have only begun to be more transparent about their decision-making.[281] The lack of transparency and defined processes around vulnerabilities equities processes (VEP) is a concern.[282] A VEP involves a careful balancing of interests in retaining a vulnerability against the risks of retaining it. The UK and several civil society organizations have argued that the presumption in such processes should be in favour of disclosure.[283] While the UN GGE Report 2021 stipulated various examples of best practices it notably fell short of endorsing a presumption in favour of disclosure.[284]

Due to the lack of clarity, as a way forward, an exchange of views about VEP and publication of VEPs, such as by UK, including relevant criteria in the process, may strengthen resilience as a CBM. Such informal guidelines may provide legal yardsticks for the balancing of conflicting interests. The UK VEP e.g. introduces operational necessity, risks of discovery by someone else, as well as possible remediation as criteria for deciding whether a vulnerability is disclosed or not.[285] In any case, the precise steps in the iterative process of disclosing and remedying vulnerabilities is complex and no international minimum standard of due diligence or an approximation of a best practice currently exists. Nevertheless, due diligence arguably requires that states at least put foreseeable and sufficiently detailed process-

281 UK, The Equities Process, 29 November 2018, available at: https://www.ncsc.gov.uk/blog-post/equities-process; see Sven Herpig/Ari Schwartz, 'The Future of Vulnerabilities Equities Processes Around the World', *Lawfare*, 4 January 2019, available at: https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world.

282 As pointed out in the UN OEWG Chairs Summary 2021 (n. 9), para. 7.

283 GCSC, 'Final Report' 2019 (n. 146), Norm 4: 'States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.'

284 UN GGE Report 2021, para. 61.

285 UK, The Equities Process 2018 (n. 281).

es in place, based on which they decide whether they retain or disclose vulnerabilities.

3.2 Information on remedies

Also with regard to the provision of remedies it is not clear whether such an obligation to provide remedies exists on the inter-state level or only in relation to the public. The NAM[286] and the UN OEWG Final Report[287] refer to notification of *users*. Such a reading would align with Art. 13 of the ILC Draft Articles on Prevention which stipulates a duty to inform the public about risky activities.[288] This inward dimension of the information requirement tentatively suggests that it should be conceived as a due diligence requirement under the duty to protect human rights but not under the harm prevention rule. Yet, once a state knows about remedies for vulnerabilities, it would be detrimental for international cyber stability if a state was entitled to withhold such information from other states. Furthermore, if, as is argued here, vulnerability disclosure is conceived as an inter-state obligation, it is only logically consequent that also informationsharing on remedies – which is an essential part of vulnerability disclosure – is owed to other states.[289] The complexities of the iterative process of sharing information about remedies in any case make it impossible to ascertain an

286 NAM Working Paper for the Second Substantive Session of the Open-ended Working Group on developments in the Field of Information and Telecommunications in the Context of International Security (UN OEWG), p. 1: 'Member States should be urged to consider the exchange of information on ICTs related vulnerabilities and/or harmful hidden functions in ICT products and to notify users when significant vulnerabilities are identified.'

287 UN OEWG Chairs Summary 2021 (n. 9), para. 25: 'States also proposed further ensuring the integrity of the ICT supply chain, expressing concern over the creation of harmful hidden functions in ICT products, and the responsibility to notify users when significant vulnerabilities are identified.'

288 ILC Draft Articles on Prevention 2001 (n. 31), art. 13: 'States concerned shall, by such means as are appropriate, provide the public likely to be affected by an activity within the scope of the present articles with relevant information relating to that activity, the risk involved and the harm which might result and ascertain their views.'

289 Arguing that sharing of remedies is an interstate obligation see Tsagourias, 'Recommendation 13j' 2017 (n. 200), para. 36, 37: 'the sharing of information about remedies, this is an interstate obligation (…) More specifically, it particularises (…) recommendation (c) on due diligence (…)'. It should be noted that the doctrinal differentiation may not be practically relevant. As soon as the public in one state

international standard, not to speak of a binding international minimum standard.

4. Links of state exploitation to attacks on the integrity of the supply chain

A closely related issue is the issue of exploitation and disclosure of ICT vulnerabilities via so-called 'attacks on the integrity of the IT supply chain'. The supply chain describes efforts to improve cyber security of IT products. In contrast to the exploitation of discovered ICT vulnerabilities attacks on the supply chain deliberately create a vulnerability already in the ICT production process. They are thus often referred to as installing 'backdoors'.[290] The *SolarWinds* hack discovered in 2020, as well as the ransomware attack exploiting a vulnerability in a Kaseya software in July 2021[291], highlighted the increasing interest of malicious cyber actors in such attacks on the integrity of the supply chain. Experts have underlined that attacks on the supply chain are particularly hideous and dangerous as they not only exploit technical vulnerabilities but affect the trust between customers and businesses and trust in the patching cycle process which is essential to increase cyber resilience.[292] Due to suspicions that the decision-making on technical standards is used for enabling the insertion of 'backdoors', the allegedly merely technical process of standard-setting in international fora has repeatedly become severely contested.[293]

---

is informed about remedies, other states will regularly acquire knowledge of the remedies as well.

290 Kim Zetter, 'Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers', *VICE*, 25 March 2019, available at: https://www.vice.com/en/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers.

291 Kellen Browning, 'Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack', *New York Times,* 2 July 2021, available at:https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html.

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

293 Dennis Broeders, *The Public Core of the Internet* (Amsterdam University Press 2015), 46: Those protocols may well be technical or logical in nature, but that does not make them immune to interests, politics and power (…) For every protocol

5. The protection of the integrity of the supply chain in the UN GGE Report 2015

Para. 13 lit. i of the UN GGE Report 2015 on the integrity of supply chain asserts that:

> 'States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions'[294]

As is typical for the norms of responsible state behaviour these normative aspirations are expressly voluntary and non-binding. The formulation of para. 13 lit. i which refers to 'reasonable steps to ensure' suggests that a potential obligation is primarily a positive protective obligation. This however masks that the undermining of the supply chain is regularly incentivized from the state level and that therefore an obligation regarding this matter is a primarily negative one – not to undermine the integrity of the ICT by creating or pushing to create backdoors. This primarily negative dimension can be seen in the recommendations made by Microsoft regarding the protection of the IT integrity chain – all of which address state actors.[295] Intrusive state action also underlies the discussion around negative duties of states not to impair the public core of the internet, inter alia by hampering with technical standards.[296] Discharging this negative prohibitive dimension of para. 13 lit. i merely requires to refrain from acts that adversely affect the integrity of the supply chain.

---

that has been promoted to the status of a standard, there were alternatives that did not succeed for one reason or another.' On the power relations underlying technical protocols and standards Julie E. Cohen, 'Cyberspace As/And Space', *Columbia Law Review* 107 (2007), 210–256, at 256: 'about the visibility and scale of the power relations manifested through technical protocols and standards'.

294 UN GGE Reports 2015, para. 13 lit.i.

295 Microsoft, 'Six Proposed Norms to Reduce Conflict in Cyberspace', 20 January 2015, available at: https://www.microsoft.com/security/blog/2015/01/20/six-proposed-norms/, e.g. para. 1: States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services. In more detail on states' duties to refrain from targeting ICT companies to install backdoors Caitriona Heinl, 'Recommendation para. 13i', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 223–239, at 237, para. 38.

296 See chapter 3.C.III.

With regard to protective 'reasonable steps to ensure' the integrity of the supply chain partnering with private industry is a central requirement in order to improve resilience.[297] This may require to hold vendors accountable to ensure security of their products, but may also include the protection of encryption, or compliance with IT security standards in public procurement.[298] A further measure to contribute to the integrity of the supply chain may be the criminalization of supply chain attacks as misuse of devices.[299] While strong reasons speak for criminalization of misuse as the required international minimum standard more *opinio iuris* would be required to elevate it to the level of a binding due diligence requirement.[300]

6. Emergence of best practice standards regarding ICT vulnerability disclosure

The overall picture regarding international law on vulnerability disclosure processes and remedies is hence murky – or in the words of Canada a 'diversity of views on the matter'[301] exist. The statements highlight an increasing awareness that vulnerability disclosure is important for a more secure cyberspace. Yet, it is so far largely unclear which institutional and procedural measures states need to adopt to address this issue and whether such measures are owed to other states, derive from the harm prevention rule, from the duty to protect under human rights law or from a self-standing duty. State practice and commentators however point to emerging best practice standards. While the evolving best practices are only *soft law* and not a binding due diligence requirement the ongoing dialogue and exchange of such practices and relevant criteria, e.g. as a CBM, may harden over time to more stringent normative commitments and contribute to clarifying normative expectations. In developing best practice templates,

297 Canada, Canada's implementation of the 2015 GGE norms 2019 (n. 166), p. 13.
298 Heinl, 'Recommendation 13i' 2017 (n. 295), para. 38.
299 Microsoft, International Cybersecurity Norms, p. 13: 'States should establish processes to identify the intelligence, law enforcement, and financial sanctions tools that can and should be used against governments and individuals who use or intend to use cyber weapons in violation of law or international norms.' On the connection between para. 13i, j and criminal prosecution Heinl, 'Recommendation 13i' 2017 (n. 295), para. 39; on criminalization of misuse of devices see below chapter 4.D.I.4.1.
300 See in more detail chapter 4.D.I.4.1.
301 Canada's comments on zero draft text, February 2021, p. 8.

states would also need to distinguish more clearly between the actors involved and associated normative expectations during various stages of the disclosure process, for example between vulnerability disclosures by researchers or intelligence officials to vendors, and vulnerability disclosure between different states, or processes through which patches against vulnerabilities are distributed. In any case, states' interests in exploitation of ICT vulnerabilities will continue to make the issue sensitive for states and states likely aim to preserve a certain leeway for continuing to exploit ICT vulnerabilities. At this point in time, disclosure of ICT vulnerabilities can hence not be considered a binding due diligence requirement.[302]

VI. Summary on procedural due diligence obligations

The preceding analysis has shown that several legal yardsticks regarding procedural due diligence obligations can be discerned. The normative aspiration of cooperation underlies all other procedural due diligence obligations but a general due diligence duty to cooperate as such provides insufficient normative direction. Specific cooperative due diligence obligations are more relevant in practice: Due diligence requires states to take action with regard to ongoing or imminent harmful cyber operations emanating from their territory. Due diligence arguably also requires states to warn or inform other states about risks of cyber harm emanating from their territory. It is however unclear under which circumstances such a duty is triggered and states are so far reluctant to commit to a duty to warn in cyberspace. Due diligence also requires that states cooperate in good faith for cybercrime prosecution. At the very minimum due diligence requires that states give reasons for a refusal to comply with cybercrime cooperation requests. It is plausible that rules for international cooperation on cybercrime prosecution are and will continue to be specified via binding and non-binding *lex specialis* norms, rather than via a broad due diligence standard. Lastly, there are strong reasons to assume that a due diligence duty to conduct a legally balanced VEP, as well as a duty to disclose vulnerabilities to the public and other states, is emerging. States however would need to be more forthcoming with regard to relevant legal criteria. It is so far not clear whether such a duty can be conceived under the harm prevention rule or as

302 Also rejecting the illegality under international law of non-disclosure of vulnerabilities Delerue, 'Cyber Operations' 2020 (n. 47), 373.

a self-standing duty, and furthermore if such a duty is primarily owed to the public, to other states, or to the international community.

D. Due Diligence Measures Regarding a State's Institutional Capacity

Procedural due diligence obligations often presuppose institutional safeguards. This invites to assess the second broad category of due diligence obligations: Measures with regard to a state's institutional capacity. This category may include legislative and administrative safeguard measures.[303]

I. Cybercrime legislation and prosecution

A legislative measure of extraordinary importance is the criminalization of malicious behaviour in cyberspace. Prosecuting cybercrime is a key tool to reduce cyber instability. As noted by a UN Study on Cybercrime in 2013:

> '[C]riminalization gaps in any country can create offender havens with the potential to affect other countries globally'.[304]

Due to the principle of *nullum crimen sine lege* lack of legislation on cybercrime is an impediment to prosecution of cybercrime. If a country does not enact cybercrime legislation it cannot prosecute crimes committed via ICT. Due to the dual criminality rule[305], lack of cybercrime legislation is also permanently hindering securing evidence in criminal procedures, apprehension and extradition.[306] Even when foreign countries detect the actor behind malicious cyber activities they are prevented from requesting assistance or extradition if the territorial state has no similar criminal law in place. In the case of the ILOVEYOU virus in the Philippines in 2000 the perpetrator for example was known but could not be prosecuted as no legislation on cybercrime existed at the time in the Philippines.[307] Countries in which no cybercrime legislation exists are hence an ideal safe haven[308]

303 On categories of due diligence obligations see chapter 4.B.V.
304 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 77.
305 Ibid., p. 60; the AU Convention on Cyber security explicitly refers to the double criminality rule in art. 28 (1).
306 Clough, 'Challenges of Harmonisation' 2015 (n. 211), 701, 715.
307 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 14), commentary to rule 13, p. 77, fn. 104.
308 Clough, 'Challenges of Harmonisation' 2015 (n. 211), 701.

for cyber criminals. Such cyber safe havens affect the stability of cyberspace globally.[309] Due to importance of cybercrime legislation the question arises whether due diligence may require states to enact cybercrime legislation as a measure of institutional capacity-building, and if so, which legislative measures are required.

1. Criminal legislation and prosecution as due diligence requirements

The interrelation between criminal prosecution and due diligence was highlighted by early cases on due diligence in which states were held responsible for exercising due diligence in investigating and apprehending non-state actors for injuries to aliens. In the *Janes* case the Tribunal held the Mexican government responsible for violating its 'duty of diligently prosecuting and properly punishing the offender'.[310] In the *Lotus* case, *Judge Moore* asserted:

> '[I]t is well settled that a State is bound to use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people'[311]

In the ICJ *Corfu Channel* case Judge Alvarez linked the enactment of substantive criminal law provisions to due diligence for harm prevention, referring to the necessity to criminalize acts 'to the detriment of other states or of their nationals'.[312] As asserted in the *Janes* case not only criminalization is required but also effective prosecution – or put differently in the

309 The necessity of cybercrime legislation was already underlined in UN General Assembly Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, UN General Assembly A/75/816, 18 March 2021, Annex to the Chairs summary A/RES/55/63, 22 January 2001, para. 1: 'Notes with appreciation the efforts of the above-mentioned bodies to prevent the criminal misuse of information technologies, and also notes the value of, inter alia, the following measures to combat such misuse: (a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies (…)'.

310 *General Claims Commission (Mexico-USA), Janes*, 16 November 1925, UNRIAA, vol. IV, 87.

311 PCIJ, *The Case of the S.S. Lotus (France v. Turkey)*, Dissenting Opinion by Moore, 7 September 1927, Series A, No. 10, 88.

312 ICJ, *Corfu Channel Case (United Kingdom v. Albania)*, Separate Opinion of Judge Alvarez, ICJ Reports 1949, 4, p. 44, para. 4.

words of the ICJ in *Pulp Mills* due diligence requires 'not only the adoption of appropriate rules and measures, but also a certain level of vigilance in their enforcement'.[313]

While the Tallinn Manual negated that enacting cybercrime legislation under the harm prevention rule was required in cyberspace, due to its restrictive stance on due diligence requirements[314], several states, such as Canada or the UK, have linked enactment of cybercrime legislation to the harm prevention rule.[315] In a thinly veiled reference to the due diligence rationale regarding criminal activities emanating from Russian territory the US has argued that:

> '[O]ur view is that when there are criminal entities within a country, [the country] certainly ha[s] a responsibility and it is a role that the government can play'[316]

Although the statement did not explicitly mention cybercrime legislation it is aimed at criminal prosecution which requires such legislation. This indicates that states increasingly recognize that the requirement to enact criminalization and to prosecute harmful actors is required to discharge due diligence in cyberspace.

2. Criminal legislation and prosecution under international human rights law

Also the due diligence duty to protect in human rights law may require criminal legislation and effective prosecution.[317] Effective criminal prosecution, particularly for interferences with the right to life, is stressed in the

313 ICJ, 'Pulp Mills' (n. 111), para. 197.

314 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 22), commentary to rule 7, p. 45; see also Woltag, 'Cyber Warfare' 2014 (n. 212), 101.

315 Canada's implementation of the 2015 GGE norms 2019 (n. 166), p. 4; UK, 'Efforts to Implement Norms' 2019 (n. 87), p. 6; also arguing for cybercrime legislation to discharge the duty to exercise due diligence Adamson, 'Recommendation 13c' 2017 (n. 29), p. 73, para. 36.

316 Maegan Vazquez/Allie Malloy, 'Biden will discuss recent cyber attack on meat producer with Putin in Geneva', *CNN*, 2 June 2021, available at: https://edition.cnn.com/2021/06/02/politics/biden-putin-jbs-foods-russia/index.html.

317 Krešimir Kamber, 'Substantive and Procedural Criminal Law Protection of Human Rights in the Law of the European Convention on Human Rights', *Human Rights Law Review* 20 (2020), 75–100, at 75.

jurisprudence of the ECtHR[318] and the Inter-American Court of Human Rights (IACtHR)[319], as well as by the UN Human Rights Committee.[320] Regarding the cyber context, the ECtHR affirmed the necessity of cybercrime legislation for the protection of the right privacy in the *KU/Finland* case in 2008:

> '[The] obligations [to protect] may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves (…) While the choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is, in principle, within the State's margin of appreciation, effective deterrence against grave acts, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions'[321]

Also in the *Bărbulescu* case – which concerned cyber-enabled privacy intrusions against an employee by an employer – the ECtHR reaffirmed that a state may discharge its due diligence duties to protect human rights against cyber threats via criminal legislation.[322] Regarding criminalization, due diligence requirements under the duty to protect human rights hereby concur with due diligence requirements for harm prevention.

318 ECtHR, *Case of Nikolova and Velichkova v. Bulgaria*, Judgment of 20 December 2007, Application No. 7888/03, para. 57; ECtHR, *Case of Kilic v. Turkey,* Judgment of 28 March 2000, Application no. 22492/93, paras. 62, 63; see also Baade, 'The Duty to Protect' 2020 (n. 64), 94.

319 IACtHR, *Case of Velásquez-Rodríguez v. Honduras*, Judgment of 29 July 1988, Series C No. 4, para. 174.

320 UN Human Rights Committee, General Comment No. 36 on article 6 of the International Covenant on Civil and Political Rights, on the right to life, 30 October 2018, CCPR/C/GC/36, para. 21: 'States parties must further take adequate measures of protection, (…) in order to prevent, investigate, punish and remedy arbitrary deprivation of life by private entities.'

321 ECtHR, *Case of K.U. v Finland*, Judgment of 2 December 2008, Application no. 2872/02, paras. 43, 46.

322 ECtHR, *Case of Bărbulescu v Romania*, Grand Chamber Judgment of 5 September 2017, Application no. 61496/08, paras, 115, 116.

3. Assessing international standard on cybercrime legislation and prosecution

This raises the question whether a least common denominator regarding criminalization of cybercrime can be presumed. So far no global cybercrime treaty exists. It also seems uncertain whether a global multilateral treaty on cybercrime will be concluded in the foreseeable future. After more than two years of contested negotiations an intergovernmental committee, established by the UN General Assembly to work on an international convention on cybercrime, could not agree on a draft text for an international convention' on cybercrime in its concluding session in February 2024.[323]

Yet, a number of regional cybercrime conventions are relevant for determining international standards on criminalization. Conduct under treaty law counts as state practice.[324] As the customary standard of diligence needs to be interpreted systematically within the context of other rules of international law[325] this state practice also influences the interpretation of due diligence under the harm prevention rule.

Of particular relevance is the Budapest Convention of the CoE.[326] The convention has been pitched as the international 'benchmark' and guideline for attempts to harmonize criminal law provisions.[327] Beyond the Budapest Convention, the 2014 *Malabo* Convention on Cybersecurity and

323 From the outset, it had been disputed whether a global convention on cybercrime is feasible or even desirable. Already the vote in the UN General Assembly on the Russian proposal to establish an intergovernmental committee was severely contested (79 to 60, 33 abstentions, 21 non-voting), UN General Assembly Resolution A/RES/74/247, 27 December 2019.

324 ILC, Draft conclusions on identification of customary international law, UN A/73/10, conclusion 6 (2): 'Forms of State practice include (…) conduct in connection with treaties; executive conduct, including operational conduct "on the ground"; legislative and administrative acts (…).'

325 On the need to interpret due diligence systemically within the context of other rules of international see above chapter 4.B.III.

326 Convention on Cybercrime 2001 (n. 215).

327 See already Marco Gercke, 'The Slow Wake of A Global Approach Against Cybercrime', *Computer Law Review International* 5 (2006), 140–145; see also Report of the Chairman of HLEG, ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG) to ITU Secretary-General, Dr. Hamadoun I. Touré by Chief Judge Stein Schjølberg, p. 6,7, para. 1.3, para. 1.4.: '. It is very important to implement at least Articles 2–9 in the substantive criminal law section, and to establish the procedural tools necessary to investigate and prosecute such crimes as described in Articles 14–22 in the section on procedural law.'

Data Protection of the AU[328], the Convention on Combating Information Technology Offences of 2010 of the Arab League[329], and the 2009 SCO Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security are further relevant regional cybercrime treaties.[330] The EU Directive 2013/40 'establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems'.[331] This variety of regional instruments[332] on cybercrime shows that cybercrime is the one area of international law in which states so far have been more forthcoming in committing to binding rules. Tellingly, the offences of the cybercrime treaties do not apply to state-sponsored activities[333], hence, committing to binding rules is less costly for states as their own cyber activities remain uninhibited.

3.1 Criminalization requirements under cybercrime treaties

Regarding the substantive requirements stipulated in the convention it is important to note that the various conventions do not only address core-cyber harm offences against the confidentiality, integrity and availability of ICT systems and networks, but also include provisions on computer-related offences, such as forgery and fraud, or content offences, such as xenophobia, child pornography, terrorist propaganda.[334] The following analysis

328 African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), 27 June 2014. The Convention entered into force in June 2023 after its 15th ratification.

329 Arab Convention (n. 228).

330 SCO Agreement International Information Security 2009 (n. 123).

331 EU, 2013/40 of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA Directive.

332 See also the model cybercrime laws by the Caribbean Community (CARICOM), Model Legislative Texts of Cybercrime/e-Crimes and Electronic Evidence Model legislation targeting the prevention and investigation of computer and network related crime Non-binding Commonwealth – Model Law on Computer and Computer Related Crimes, available at: https://www.unidir.org/cpp/en/multilateral-frameworks.

333 Lahmann, 'Unilateral Remedies' 2020 (n. 146), 20.

334 Convention on Cybercrime 2001 (n. 215), arts. 7–10; Arab Convention (n. 228), arts. 10–18; the AU Convention also entails provisions on data protection, see Malabo Convention (n. 328), art. 8f.

will exclude these offences from the analysis due to this study's exclusive focus on cyber harm.[335]

With regard to offences which cause cyber harm, i.e. offences that compromise the confidentiality, integrity and availability of ICT, a converging minimum standard as the bottom line has emerged. Nevertheless, states have a certain degree of flexibility to implement this minimum standard as no uniform standard can be detected.

To begin with, all regional conventions require criminalization of access operations.[336] Art. 2 of the Budapest Convention exemplarily requires:

> 'Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. (…)'[337]

The other conventions entail similar provisions on access operations.[338] Deviations exists with regard to details. In order to avoid over-criminalization the EU Directive for example excludes 'minor cases' and furthermore requires an 'infringement of a security measure'.[339] An important *de minimis* threshold for criminalization may also be the exemption of security researchers.[340] Further deviations exist with regard to aggravating circumstances. The EU Directives 2013/40 for example stipulates operations against the information systems of critical infrastructure as an aggravating circumstance.[341]

Despite such divergences as to the specific criminalization access operations are almost universally criminalized. Already in 2013 the UN Study

335 See on the concept of cyber harm of this study which excludes content harm chapter 1.B.III.

336 For a definition of access operations see UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 257: 'Refers to acts involving gaining access to computer data without authorization or justification (…) This is the case, for example, if a perpetrator illegally accesses a computer database (…) if a perpetrator, who is working for a particular company, copies files to take with him without authorization.

337 Convention on Cybercrime 2001 (n. 215), art. 2.

338 Arab Convention (n. 228), art. 6; Malabo Convention (n. 328), art. 29 (1a-c); EU Directive 2013/40 (n. 331), art. 3.

339 EU Directive 2013/40 (n. 331), art. 3. See also the Convention on Cybercrime 2001 (n. 215), art. 2: '(…) A Party may require that the offence be committed by infringing security measures (…)'.

340 On the importance of IT security researchers for the detection of ICT vulnerabilities see above chapter 4.C.V.4.1.

341 EU Directive 2013/40 (n. 331), art. 9 (4c).

found that only 7 % of surveyed states had not yet criminalized access operations.[342] This suggests that criminalizing access operations can be considered the international minimum standard. A state cannot argue that it acted diligent if it has not criminalized access operations.

Aside from access operations, also interception of communications between ICT users or generally of data in transfer can compromise the confidentiality of data exchange processes.[343] Interception may occur directly through computer systems or indirectly, e.g. through technical devices fixed to transmission lines, or through the use of software.[344] Attackers usually search for weak entry points regarding transmitted communication points, for instance wireless connections.[345] While access operations are primarily directed at stored data interception abuses the particular vulnerability of data in transmission. Interception is particularly relevant with regard to cloud storage, and email transmissions which are particularly vulnerable.[346]

All multilateral treaties entail provisions requiring criminalization of interception of computer data.[347] 95 % of states surveyed in the UN Comprehensive Study on Cybercrime in 2013 had criminalized interception of computer data in their domestic law. The largely homogeneous criminalization of interception is however not tantamount to a uniform international standard. States' legislation is for example structured differently. Some states have enacted a cyber-specific provision on interception, other have included it in a general offence.[348] Despite such divergences in details, criminalization of the interception of non-public transmissions of computer data can be considered the international standard and a state is negligent if interception of data transfer in cyberspace is not criminalized in its domestic law.

Further offences which cause cyber harm are data and system interference. Both are interrelated. If a cyber operation affects the integrity and availability of computer data, it constitutes data interference. As data is non-tangible, interference with data is frequently not covered by traditional

342 UN ODC, 'Comprehensive Study' 2013 (n. 214).
343 ITU, Understanding Cybercrime: Phenomena, Challenges and Legal Response (ITU: September 2012), p. 19.
344 See CoE, 'Explanatory Report' (n. 238), p. 10, para. 53.
345 ITU Understanding Cybercrime 2012 (n. 343), p. 20.
346 Ibid., p. 19.
347 Convention on Cybercrime 2001 (n. 215), art. 3; Arab Convention (n. 228), art. 7; Malabo Convention (n. 328), art. 29 (2a); EU Directive 2013/40 (n. 331), art. 6.
348 UN ODC, 'Comprehensive Study' 2013 (n. 214),p. 78.

criminal law provisions on damage to physical objects.[349] As data interference may impair the smooth operation of software or computer systems[350], it may thereby amount to system interference.[351] A means to interfere with computer data is e.g. ransomware which allows an offender to encrypt files and deny access to victims unless they pay a ransom to decrypt the files.[352] Also computer worms – replicating programs that can initiate data-transfer processes within a network – or DDoS operations, may interfere with computer data and computer systems.[353] The effects of data and system interference are often graver than access and interception offences as not only the confidentiality of data, but also its integrity and availability may be affected, leading to potentially disruptive or even destructive physical consequences.[354]

It is hence unsurprising that all cybercrime treaties require the criminalization of data and system interference.[355] Consequently, the overwhelming majority of states have enacted criminal legislation.[356] The regional norms slightly differ with regard to the necessity of harm, or damage as a consequence of data interference. Both the Budapest Convention and the EU Directive for example exclude criminalization of minor cases.[357] In several domestic legislations data and system interference are criminalized via a single offence.[358] Similar to criminalization of access and interception operations state practice is hence largely homogeneous, despite divergences on details. Furthermore, no state has taken an explicit or implicit stance

349 Ibid., p. 88.
350 Ibid.
351 For examples of system interference, e.g. operations against CNN, Amazon or eBay, with severe disruptive potential see ITU Understanding Cybercrime 2012 (n. 343), p. 20.
352 Ibid.
353 Ibid.
354 On different degrees of cyber harm see chapter 1.C.
355 Convention on Cybercrime 2001 (n. 215), art. 4; Arab Convention (n. 228), art. 8; Malabo Convention (n. 328), arts. 29 (2b), (2d); EU Directive 2013/40 (n. 331), arts. 4, 5.
356 See e.g. Criminal Law of the People's Republic of China, arts. 285–287; US, Computer Fraud and Abuse Act, 18 United States Code 1030, 1986; Argentina, Cybercrime and Violation of Privacy Act, Law no. 26.388; German Criminal Code, sections 303a, 303b; see for further references Coco/Dias, 'Cyber Due Diligence Report' 2021 (n. 129), 215.
357 EU Directive 2013/40 (n. 331), art. 5: '(…) at least for cases which are not minor'; Convention on Cybercrime 2001 (n. 215), art. 4.
358 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 89.

against criminalization of data and system interference. In particular, no state has argued that a requirement would impede its sovereignty or that it would exceed its capacity. A state hence acts negligent if it does not criminalize data and system interference.

More difficult is the assessment of the development and sale of 'software tools' which exploit vulnerabilities or weaknesses in the design of ICT. Production, possession and distribution of such software tools is an increasingly profitable business.[359] In the context of cybercrime treaties, it is frequently framed as 'misuse of devices'.[360] The private Israeli company NSO is a prominent example of a company developing 'software tools' to exploit ICT vulnerabilities and selling them to interested state parties.[361]

International legal practice has increasingly pushed towards illegalizing such activities. Para. 13 lit. i of the UN GGE Report 2015 for example asserts:

> '(…) States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions'[362]

The Budapest Convention and the Arab League Convention require criminalization of 'misuse of devices'.[363] Already in 2013, the majority of countries surveyed in a UN study had criminalized the misuse of devices.[364] Yet, divergences exist as to whether possession, creation, distribution and use is generally criminalized or only some of these acts.[365] The conventions provide for exceptions to the requirement to criminalize. The Budapest Convention for example adds 'without right' as an additional requirement

359 See above chapter 4.C.V.

360 The UN Study refers to misuse of devices as 'development or distribution of hardware or software solutions that can be used to carry out computer or internet-related offences', see UN ODC, 'Comprehensive Study' 2013 (n. 214), Annex One: Act Descriptions, p. 257.

361 'Cyber-surveillance weapon' 2021 (n. 264); see also Mehul Srivastava, 'WhatsApp voice calls used to inject Israeli spyware on phones', *Financial Times*, 14 May 2019, available at: https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab.

362 UN GGE Report 2015, para. 13 lit. i.

363 Convention on Cybercrime 2001 (n. 215), art. 6; Arab Convention (n. 228), art. 8; Malabo Convention (n. 328), Art. 29 (1h); EU Directive 2013/40 (n. 331), art. 7.

364 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 81.

365 Ibid.

for criminalization[366], similar to Art. 7 of the EU/2013/40.[367] The Explanatory Notes clarify that this means that criminalization is not required when the activity is conducted for 'legitimate purposes'.[368] Arguably, 'legitimate purposes' could be law enforcement or intelligence purposes. In this reading, selling ICT 'weapons' to governments by a private company may be exempted from the criminalization requirement.[369] Further restrictions on criminalization exist. Some states e.g. only criminalize the production and distribution of software tools when the software is used to commit a crime or when it is exclusively designed to commit a crime.[370] This ambiguous picture regarding the criminalization of 'misuse of devices' is concerning: Software tools exploiting the vulnerability of ICT create cyber instability.[371] Selling software tools to authoritarian countries makes it all but certain that human rights safeguards for intercepting and surveilling will be disregarded[372], and may furthermore affect the integrity of the supply chain. While treaty norms, the majority of state practice and the normative aim of para. 13 lit. i of the UN GGE Report 2015[373] suggest that states should severely curtail exemptions to criminalization, state practice, so far, is not sufficiently consistent to assume that this is the required standard of due diligence.

366 UN ODC, 'Comprehensive Study' 2013 (n. 214), art. 6.

367 EU Directive 2013/40 (n. 331), art. 7: 'the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right (…)'.

368 CoE, 'Explanatory Report' (n. 238), paras. 76, 77.

369 The private Israeli firm NSO openly admits to selling 'spyware' and further hacking tools to governments, see 'Pegasus: Spyware sold to governments 'targets activists'', *BBC,* 19 July 2021, available at: https://www.bbc.com/news/technology-57881364.

370 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 257.

371 See above chapter 4.C.V.

372 The revelations around the so-called 'Pegasus'project are a case in point, see Cybersurveillance weapon' 2021 (n. 264).

373 UN GGE Report 2015, para. 13i: 'States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions'; in more detail see above chapter 4.C.V.7.

3.2 Convergence on an international minimum standard

Due to the convergence between the various regional treaties and state practice criminalization of access, interception operations and system and data interference it can be assumed that due diligence requires criminalization of such activities. Regarding the criminalization of misuse of devices states are more permissive and allow for various exemptions to criminalization. States are however at least required to generally criminalize the distribution and sale of vulnerability-exploiting software tools.

Assuming that due diligence requires criminalization of such activities is not tantamount to assuming a uniform international standard. Divergences exist with regard to details, such as *de minimis* exclusion, or systematic divergences within the structure of domestic criminal law. Also the specificities of a domestic criminal system, e.g. regarding intent, omission, attempt, negligence etc. preclude a uniform international standard.[374] It is hence clear that the international minimum standard does not require identical laws.[375] Criminalization however needs to ensure that the criminal legislation on these core cyber offence is not lax or inadequate.[376] Relegating criminalization of core cybercrime offences to mere voluntary guidelines would not give justice to the homogeneous state practice and the importance of eliminating cyber safe havens for global cyberspace.

4. Criminal procedural law as a due diligence requirement

Cybercrime legislation as such would largely lack teeth, if there would be no means to enforce it via criminal procedural law. In order for cybercrime legislation to have a deterrent effect with a preventive impact it is necessary to enact criminal procedural laws, and to implement them.[377]

The necessity of enacting criminal procedural legislation was already highlighted by a resolution of the UN General Assembly in 2000 which addressed the necessity of introducing procedural measures to address the problem of securing and accessing evidence in cybercrime matters, in particular electronic data. It stated that:

374 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 79.
375 Clough, 'Challenges of Harmonisation' 2015 (n. 211), 701.
376 See this formula in General Claims Commission, 'Janes' (n. 310).
377 GCSC, 'Final Report' 2019 (n. 146), p. 24.

> 'Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations'.[378]

The UN Comprehensive Study of 2020 asserted that it was 'imperative to develop adequate (…) data retention/data preservation rules'.[379] Scholars have assumed that due diligence requires the 'establishment of investigative cyber capabilities[380] and have linked due diligence to prosecution.[381] Also Canada has explicitly linked its enactment of cybercrime legislation and criminal procedural legislation regarding cyber offences to the harm prevention rule.[382]

4.1 Standard procedural measures

As data storage is costly, stored computer data is often stored only temporarily by internet service providers, at times only seconds, minutes, hours, days or weeks. Frequently, domestic legislation also requires the erasure of data by default immediately or after some period of time, inter alia for the protection of privacy.[383] In criminal investigations of cybercrime it is hence often problematic that some data is not accessible after a certain period of time.

Thus, in order to secure data for potential investigations, all agreements on cybercrime entail provisions on expedited preservation of computer data.[384] Accordingly, the vast majority of states has enacted legislation on

378 UN General Assembly Resolution A/RES/55/63, 22 January 2001, para. F.
379 UN Study, Draft Report, 29 July 2020, UNODC/CCPCJ/EG.4/2020/L.1/Add.1, para. 33.
380 Monnheimer, 'Due Diligence' 2021 (n. 36), 189.
381 Matthew Sklerov, 'Solving the Dilemma of State Response to Cyberattacks', *Military Law Review* 201 (2009), 1–85, at 13; Adamson, 'Recommendation 13c' 2017 (n. 29), p. 73, para. 36.
382 Canada's implementation of the 2015 GGE norms 2019 (n. 166), p. 4.
383 On the normative aim to save personal data for the shortest time possible, EU General Data Protection Regulation (EU) 2016/679 (GDPR), 27 April 2016, art. 5 (1e): 'Personal data shall be (…) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (…)'; Rc. 39.
384 Convention on Cybercrime 2001 (n. 215), art. 16; Arab Convention (n. 228), art. 23; Malabo Convention (n. 328), Art. 31 (3e).

expedited preservation of data.[385] Furthermore, the major cybercrime treaties require legalizing orders for computer data, hereby enabling that data is not only preserved but also obtained by law enforcement authorities.[386] All cybercrime treaties also require legalization of real-time collection of traffic data interception of content data.[387] While the vast majority of states has implemented legalizing such measures still a substantial amount has not yet done so, despite the 'fundamental' need to rely on such data in investigations.[388]

Nevertheless, state practice suggests that establishing legislation on four cyber investigative capabilities – preservation of data, order to obtain preserved data, interception of traffic and content data – can increasingly be considered the international standard. Yet, two aspects call into question whether it is promising to conceive the establishment of such capabilities as a due diligence requirement.

4.2 Divergences regarding human rights safeguards

With regard to criminal procedural it is important to point out that a uniform due diligence standard is unrealistic and even undesirable from the outset. A uniform standard regarding preservation of data risks leading to a race to the bottom for human rights safeguards in criminal procedural law. Already the preservation of data interferes with the right to privacy. Mindful of the risks of investigative capabilities for privacy the UN General Assembly Res. 68/167 on the right to privacy in the digital age required states to 'review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data' with a view to protecting privacy'.[389] Also the UN Human

385 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 128; see e.g. Jamaica, The Cybercrimes Act 2015, no. 31, section 14; Kenya, Computer Misuse and Cybercrimes Act 2018, sec. 51; US, 18 United States Code, Crimes and Criminal Procedure, § 2703(f).

386 UN ODC, 'Comprehensive Study' 2013 (n. 214), 122.

387 Convention on Cybercrime 2001 (n. 215), art. 20, 21; Arab Convention (n. 228), art. 29; Malabo Convention (n. 328), Art. 31 (3a-c).

388 UN ODC, 'Comprehensive Study' 2013 (n. 214), 128.

389 UN General Assembly, 'Right to privacy in the digital age' 2013 (n. 36), para. 4c: 'Calls upon all States (…) (c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a

Rights Council Res. 26/13 and the UN GGE Report 2021, as well as e.g. Canada[390], have highlighted that addressing security concerns and gathering of evidence in cyberspace needs to comply with international human rights law and other rules of international law generally.[391] The need to assess human rights-compliance of cyber investigative measures seems particularly acute as measures, such as data retention or interception, may also be applied beyond the cyber context with regard to general offences.[392] It is hence important to enact human rights safeguards regarding criminal procedural measures. Such safeguards could for example be restrictions of more intrusive measures, such as interception of content or traffic data, to graver crimes or to ensure judicial authorization or review of procedural measures, or to require due care in investigations.[393]

The extent to which states have implemented such human rights safeguards in state practice deviates. Art. 15 of the Budapest Convention requires 'adequate protection of human rights and liberties'.[394], By contrast, the Arab League Convention on Cybercrime concerningly does not include provisions on human rights safeguards. Also the Malabo Protocol contains only very little rules for criminal procedure and no human rights safe-

---

view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law.'

390 UN OEWG Chairs Summary 2021 (n. 273), Annex, Canada, p. 12.

391 UN GGE Report 2021, para. 33: '(…) States are also encouraged to develop appropriate protocols and procedures for collecting, handling and storing online evidence relevant to criminal and terrorist use of ICTs and provide assistance in investigations in a timely manner, ensuring that such actions are taken in accordance with a State's obligations under international law'; UN Human Rights Council, 'Human Rights on the Internet' 2014 (n. 63), para. 5: 'Calls upon all States to address security concerns on the Internet in accordance with their international human rights obligations to ensure protection of freedom of expression, freedom of association, privacy and other human rights online (…)'.

392 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 124. Draft art. 23 (2c) of the currently negotiated international convention on cybercrime e.g. requires states to apply its procedural measures for 'any criminal offence', UN GA, Revised draft text of the convention, A/AC.291/22/Rev.1, 6 November 2023, draft art. 23 (2c); highly critical regarding this aspect from the perspective of human rights Tomaso Falchetta, 'The Draft UN Cybercrime Treaty Is Overbroad and Falls Short On Human Rights Protection', *JustSecurity*, 22 January 2024, available at: https://www.justsecurity.org/91318/the-draft-un-cybercrime-treaty-is-overbroad-and-falls-short-on-human-rights-protection/.

393 Ibid., p. 134–136; Sven Herpig, *A Framework for Government Hacking in Criminal Investigations* (Stiftung Neue Verantwortung 2018), p. 21.

394 Convention on Cybercrime 2001 (n. 215), art. 15-.

guards.[395] The UN Study of 2013 noted that 15 % of countries replying to a questionnaire had no safeguards for protection of privacy, and human rights more generally, in place.[396] Due to the intrusiveness of some investigatory measures, such a lack of safeguards almost certainly leads to violations of human rights. Even within like-minded countries, such as the EU, divergences regarding procedural safeguards in criminal investigations exist.[397] Due to these divergences regarding human rights safeguards it seems futile to assume an international legal standard for investigative capabilities. Tellingly, the negotiations on an international convention on cybercrime reached a deadlock inter alia due to divergent positions on human rights safeguards and the principle of proportionality.[398] Even if states could agree on the principles of necessity, subsidiarity and proportionality regarding investigative measures, the margin of appreciation of implementing is so wide that it is also hard to point to an internationally recognizable best practice standard. Due to these wide divergences it should be cautioned against a uniform due diligence data preservation standard as such a standard may trigger an overzealous and human rights-violating implementation.

4.3 Diverging capacities

A further concern against assuming a binding due diligence standard for cyber investigative capabilities is the diverging technological capacity of states. The vast majority has indicated that it may require technical assistance in cybercrime prosecution.[399] Divergences in capacity were initially also a problem in Europe.[400] Some states face significant capacity problems

395 Malabo Convention (n. 328), art. 31 (3).
396 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 136.
397 De Busser, 'Recommendation 13d' 2017 (n. 119), para. 4: 'The significant difficulties (…) on the level of the EU when making efforts to harmonize substantive and procedural criminal law of the member states, demonstrate that this is an objective that should not be underestimated'. On the complexity of ECJ cases on data retention and collection with ramifications for cross-border data transfer see Christakis/Terpin, 'Law enforcement access to data' 2021 (n. 212), 25.
398 Alexis Steffaro, 'Detour or Deadlock? Decoding the Suspended UN Cybercrime Treaty Negotiations', 4 March 2024, available at: https://www.centerforcybersecuritypolicy.org/insights-and-research/detour-or-deadlock-decoding-the-suspended-un-cybercrime-treaty-negotiations.
399 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 178.
400 Clough, 'Challenges of Harmonisation' 2015 (n. 211), 725, fn. 252.

or have insufficient technology.[401] As a result, technologically less developed states may shy away from signing the Budapest Convention because they are unable to comply with the procedural requirements, e.g. on interception of traffic or content data.[402] The slow ratification of the AU Malabo Protocol may, inter alia, have been due to concerns over insurmountable capacity limits.[403]

Instead of asserting uniform due diligence standard on investigative capabilities it seems hence more worthwhile to focus on capacity-building and technical assistance[404], for example through training 'sufficient training of investigators, prosecutors and judges'.[405] Several states underlined that capacity-building is crucial to foster international cooperation for cybercrime prosecution in the ongoing UN Comprehensive Study.[406]

4.4. The gradual emergence of an international minimum standard and associated risks

The establishment of investigative cyber measures on data preservation, ordering of data and interception can increasingly be considered the predominant international standard. Due to diverging capacities it can however so far not be considered a binding due diligence requirement. Framing the establishment of investigative cyber capabilities as a binding due diligence requirement may furthermore prove counterproductive: It risks to incentivize the excessive extension of investigative capabilities which disregard the requirements of necessity, subsidiarity and proportionality under international human rights law.

401 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 123, 152, 172.
402 Clough, 'Challenges of Harmonisation' 2015 (n. 211), 725.
403 Ibid.
404 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 178.
405 Expert Group Report 2019 (n. 253), p. 3, para. 10 lit.b: '(…) other Member States suggested that it was not necessary or appropriate to consider a new global legal instrument because the challenges posed in respect of cybercrime and the sufficient training of investigators, prosecutors and judges were best addressed through capacity-building, active dialogue and cooperation among law enforcement agencies (…)'.
406 Ibid.

II. Level of actual or constructive knowledge under the harm prevention rule

In order to hold a state accountable under the due diligence standard it is necessary that the state had knowledge of the harmful activity.[407] Yet, when is a state expected to have known, or in the words of ICJ Judge Alvarez in *Corfu Channel* – when does a state have a 'duty to have known'[408] in cyberspace? Which proactive steps of institutional capacity-building does due diligence require from states to acquire knowledge?

1. No rebuttable presumption of knowledge

The mere fact that a cyber operation is emanating from a state's territory neither implies that the state knew or that it ought to have known of it, nor creates a rebuttable presumption that it knew. As the ICJ stated in *Corfu Channel*:

> '[I]t cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known'[409]

In cyberspace, the UN GGE Report 2015 similarly asserted:

> '[T]he indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State.'[410]

While the reference concerns attribution it also suggests that it is insufficient to attribute knowledge based on the mere fact that a cyber operation emanated from a state's territory as attribution also requires knowledge of

407 See chapter 2.A.IV; see also Giulio Bartolini, 'The Historical Roots of the Due Diligence Standard', in Heike Krieger/Anne Peters/Leonhard Kreuzer (eds.), *Due Diligence in the International Legal Order* (Oxford: Oxford University Press 2020), 23–41, at 38.

408 ICJ, Separate Opinion of Judge Alvarez (n. 312), p. 44, para. 4.

409 ICJ, *Corfu Channel Case (United Kingdom v. Albania)*, Judgment of 9 April 1949, ICJ Reports 1949, 4, p. 18.

410 UN GGE Report 2015, para. 28f.

the relevant facts.[411] Hence, in line with the ICJ judgment in *Corfu Channel,* the fact that a cyber operation emanated from the territory of a state does not create a rebuttable presumption that the state knew.[412]

2. Duty to have known under the harm prevention rule

It would however be inadequate if a state could merely point to its lack of actual knowledge regarding the harmful activity and hereby evade accountability. The ICJ asserted in *Corfu Channel*:

> '[T]hat a State on whose territory or in whose waters an act contrary to international law has occurred, may be called upon to give an explanation. […] [A] State cannot evade such a request by limiting itself to a reply that it is ignorant of the circumstances of the act and its authors'.[413]

Hence, states are held accountable for what they know, but also for what they should know. Judge *Alvarez* asserted this in his Separate Opinion in the case:

> '[E]very State is considered as having known, or as having a duty to have known, of prejudicial acts committed in parts of its territory where local authorities are installed; that is not a presumption, nor is it a hypothesis, it is the consequence of its sovereignty.'[414]

Alvarez hereby expresses the 'constructive knowledge' rationale based on which a state's knowledge is imputed, regardless of whether actual knowledge existed. This is justified as knowledge was obtainable through the exercise of available means, in this case through installed authorities.[415] In a similar vein, the ILC reiterated in its commentaries to the Draft Articles on Prevention that a state needs to take 'reasonable efforts to inform itself of

411 ILC, Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), UN General Assembly, A/56/10, 23 April-1 June, 2 July-10 August 2001, commentaries to art. 2, p. 35, para. 4.

412 Coco/Dias, 'Cyber Due Diligence' 2021 (n.63), 789; however arguing for such a rebuttable presumption Wolf Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace', in Christian Czosseck/Rain Ottis/Katharina Ziolkowski (eds.), *International Conference on Cyber Conflict* (2012) 7–19, at 17.

413 ICJ, *Corfu Channel* (n. 409), p. 18.

414 ICJ, Separate Opinion of Judge Alvarez (n. 312), p. 44, para. 3.

415 See chapter 2.A.IV.

factual and legal components that relate foreseeably to a contemplated procedure (…)'.[416] It also stated that due diligence requires taking appropriate measures to identify risky activities.[417]

Acquiring knowledge about the risk of harm can also be a due diligence requirement under the duty to protect in international human rights law. The ECtHR for example required the establishment of observation posts to enable the state to warn the public about impending, possibly life-threatening dangers.[418] The UN Human Rights Committee noted that 'supervision' may be required in order to prevent and punish perpetrators.[419] It is hence clear that due diligence for harm prevention, as well as due diligence under human rights law, may require states to proactively acquire knowledge about potentially risky behaviours.

States have broadly recognized that the constructive knowledge standard applies in cyberspace. The Netherlands for example acknowledged the applicability of the constructive knowledge standard.[420] Also a report of the CoE pointed at monitoring measures for discharging due diligence obligations – or in the words of the report 'reasonable efforts by a state to inform itself of factual and legal elements'.[421] Moreover, the UN GGE Report 2021 recognized that due diligence may require states to acquire information.[422] Only New Zealand explicitly advocated against the applicability of the constructive knowledge standard and argued that only in the case of actual

416 ILC Draft Articles on Prevention 2001 (n. 31), commentary to art. 3, p. 154, para. 10.
417 Ibid.
418 ECtHR, *Case of Budayeva and Others v. Russia*, Judgment of 20 March 2008, Application Nos 15339/02 et al., para. 156.
419 UN Human Rights Committee, 'General Comment 36' (n. 76), para. 21.
420 Netherlands, 'International Law in Cyberspace' 2019 (n. 32), p. 4.
421 Steering Committee on the Media and New Communication Services (CDMC), Explanatory Memorandum to the draft Recommendation CM/Rec(2011) of the Committee of Ministers to member states on the protection and promotion of Internet's universality, integrity and openness, CM(2011)115-add1 24 August 2011, para. 82. The reference was made in relation to the 'universality and integrity of the Internet' but it supports the argument that also in the cyber context due diligence may require best efforts to acquire information.
422 UN GGE Report 2021, para. 29: 'This norm reflects an expectation that if a State is aware of or is notified in good faith that an internationally wrongful act conducted using ICTs is emanating from or transiting through its territory it will take all appropriate and reasonably available and feasible steps to detect, investigate and address the situation'.

knowledge a state would be required to act with due diligence.[423] It provided no further reason for its position, but the context of the statement suggests that New Zealand was concerned about a potential push towards extensive monitoring of cyber activities.[424] Yet, the question if and to which degree a state needs to monitor cyber activities is a secondary question and requires careful balancing[425] that should not be precluded by negating the constructive knowledge standard from the outset. Hence, it can be assumed that constructive knowledge suffices in cyberspace and that, consequently, due diligence may require states to acquire knowledge.[426]

3. Content of a duty to have known in cyberspace

Constructive knowledge is defined as 'knowledge that one using reasonable care and diligence should have, and therefore is attributed by law to a given person [or State]'.[427] The UN GGE 2021 highlighted that states are not required to 'monitor all cyber activities'[428], hereby reflecting the scepticism of New Zealand regarding the constructive knowledge standard. It stated that:

> 'The norm raises the expectation that a State will take reasonable steps within its capacity to end the ongoing activity in its territory through means that are proportionate, appropriate and effective and in a manner consistent with international and domestic law. Nonetheless, it is not expected that States could or should monitor all ICT activities within their territory.'[429]

423 New Zealand, The Application of International Law to State Activity in Cyberspace, 1 December 2020, para. 17.
424 Ibid.
425 On the requirement to interpret due diligence in compliance with other international legal rules, including human rights law, see above chapter 4.B.III.
426 Karine Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations' *Baltic Yearbook of International Law* 14 (2014), 23, 28; Coco/Dias, 'Cyber Due Diligence' 2021 (n. 63), 793.
427 Bryan A. Garner, in Henry Campbell Black (founder), *Black's Law Dictionary* (St. Paul (MN): West Publishing 10th ed. 2014).
428 New Zealand, 'International Law in Cyberspace' 2020 (n. 423); para. 17; Bannelier/Christakis, 'Prevention Reactions' 2017 (n. 151), p. 20.
429 UN GGE Report 2021, para. 30a.

Similarly, Ecuador argued in its UN OEWG 2020 submission that

> 'this norm should not be interpreted as requiring a state to monitor proactively all ICTs within its territory'.[430]

With regard to authoritarian tendencies to exercise strict control over cyberspace and in particular strict content control, concerns of over-monitoring via an extensive interpretation of due diligence requirements seem well-founded. Yet, they should not be overemphasized.[431] As the ICJ stated in *Bosnia Genocide:*

> 'It is clear that every State may only act within the limits permitted by international law'[432]

Hence, a due diligence duty to acquire information about risks of harm would need to be interpreted in compliance with other rules of international law, in particular with human rights law. As a duty to monitor *all* ICT would violate international human rights law[433] due diligence does not require such monitoring.

Yet, ending the subject matter at this point, as is often done, does not seem satisfactory. It is worthwhile to analyse circumstantial evidence that courts have accepted in order to conclude on which level of knowledge a state ought to have in cyberspace.

In the *Corfu Channel* case based its assumption of constructive knowledge inter alia on the fact that Albania was monitoring its territorial waters closely.[434] In the *Bosnia Genocide* case the ICJ Judge *Keith* considered a number of criteria and specific circumstances, like overall role and specific relationships of various actors, in order to conclude that Miloševic on behalf of the Serbian state 'must have known'. These examples make clear that circumstantial evidence may suffice and that various international tribunals have shown leniency and 'liberal recourse to interferences of fact and circumstantial evidence'.[435]

430 Ecuador, 'Preliminary comments' 2020 (n. 192), p.2.
431 Buchan, 'Obligation to Prevent' 2016 (n. 88), 442.
432 ICJ, 'Bosnia Genocide' 2007 (n. 39), para. 430; see also above chapter 4.B.III.
433 Buchan, 'Obligation to Prevent' 2016 (n. 88), 442; Delerue, 'Cyber Operations' 2020 (n. 47), 362.
434 ICJ, *Corfu Channel* (n. 409), p. 18, 19: 'It is clearly established that the Albanian Government constantly kept a close watch over the waters of the North Corfu Channel'.
435 Monnheimer, 'Due Diligence ' 2021 (n. 36), 121; ICJ, *Corfu Channel* (n. 409), p. 18.

Applying such circumstantial evidence in the cyber context, one may argue that a significant increase in bandwidth[436] may indicate that a state ought to have known. Further criteria may be that a certain commonly known signature was used[437], unusual password activity[438], unusually huge data transfers, unusual traffic data[439], or an unusual range of IP addresses used.[440] Furthermore, the organizational proximity of a state to an actor, e.g. an intelligence unit, may be considered a relevant factor in attributing constructive knowledge, regardless of the question whether actions of such actors can be attributed or if a state is complicit in it. Other circumstantial evidence may be that a state routinely operates investigative measures that should regularly detect the malicious operation in question[441], that governmental infrastructure was used[442], or that it in a specific case conducted a law-enforcement measure.[443]

4. Practical implications

In practice, this requires that a state uses the channels of acquiring knowledge that it already has in place.[444] In doing so, it needs to comply with other rules of international law.[445] Divergences between states are likely as 'active anticipation and constant vigilance' can be cost-intensive.[446] Developing states may lack the technological capacity to acquire knowledge in

436 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 14), commentary to rule 6, p. 41, para. 40.
437 UK, Department for Business Innovation & Skills, Guidance, 10 Steps: Monitoring, 16 January 2015, available at: https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-monitoring--11.
438 US, National Institute of Standards and Technology (NIST), Manufacturers Guide to Cybersecurity, For Small and Medium-Sized Manufacturers, 2019, p. 21.
439 Delerue, 'Cyber Operations' 2020 (n. 47), 161.
440 UK, 10 Steps Monitoring (n. 437).
441 Buchan, 'Obligation to Prevent' 2016 (n. 88), 440.
442 Luke Chircop, 'A Due Diligence Standard of Attribution in Cyberspace', *International and Comparative Law Quarterly* 67 (2018), 1–26, at 8.
443 Lahmann Unilateral Remedies' 2020 (n. 146), 158.
444 Coco/Dias, 'Cyber Due Diligence' 2021 (n.63), 788; Delerue, 'Cyber Operations' 2020 (n. 47), 362; in so far concurring with ICJ, Separate Opinion of Judge Alvarez (n. 312), p. 44, para. 4.
445 Coco/Dias, 'Cyber Due Diligence' 2021 (n. 63), 789.
446 Stoyanova, 'Positive Obligations' 2020 (n. 71), 608.

cyberspace.[447] It is hence compulsory that states press ahead with capacity-building to keep technologically up to date.[448]

Furthermore, taking legislative measures is a measure that every state, regardless of capacity, can take.[449] States could set up channels for gaining knowledge, for example by stipulating domestic obligations to report or notify about cyber security incidents. Examples are the EU NIS 1 and NIS 2 directives which require member states to ensure that critical infrastructure operators report, without undue delay, incidents having a substantial impact on their services to the incident response teams or competent authorities.[450] Member states are also required to ensure that non-essential service providers are under an obligation to report incidents when they have a 'substantial impact'.[451] Reporting requirements of critical infrastructure operators are also recommended by international institutions.[452] Acquisition of knowledge could furthermore be achieved via legislation on retention and preservation of data in criminal proceedings. In this regard the due diligence requirement to acquire knowledge may converge with the due diligence requirement to put cyber investigative capabilities in place.[453] As state practice and opinio iuris so far is not sufficiently consistent these examples of acquiring knowledge, as well as the requirement to press ahead with technological capacity-building, is currently rather to be considered best practice. Yet, as the bottomline, due diligence requires that states at least set up a basic infrastructure, via legislative and administrative measures, that brings them into the position to acquire knowledge of harmful

447 Eric Talbot Jensen/Sean Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?', *Texas Law Review* 95 (2017), 1555–1577, at 1574.

448 Coco/Dias, 'Cyber Due Diligence' 2021 (n. 63), 794.

449 ILC Draft Articles on Prevention 2001 (n. 31), commentaries to art. 3, p. 155, para. 17: 'Vigilance, employment of infrastructure and monitoring of hazardous activities in the territory of the State, which is a natural attribute of any Government, are expected.'

450 EU, NIS 2 directive (n. 275), art. 23 (1); see also already before the repealed directive EU, Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS 1 directive), art. 14 (3).

451 NIS 2 directive (n. 275), art. 23 (1); before already NIS 1 directive (n. 450), art. 16 (3).

452 ITU, Guide to Developing a National Cybersecurity Strategy, 2018, p.25.

453 See above chapter 4.D.I.5.1.

cyber activities and to hereby 'keep being informed' about activities on their territory.[454]

III. Critical infrastructure protection

States are highly concerned about cyber harm to critical infrastructure.[455] As a measure of institutional capacity-building, due diligence may require states to protect their *own* critical infrastructure against risks of cyber harm.

1. Duty to protect own critical infrastructure against cyber harm

Para. 13 lit. g of the UN GGE Report 2015 stipulates that states should protect *their* critical infrastructure.[456] This norm was endorsed by the UN General Assembly[457], and similarly reasserted in the UN OEWG.[458] Despite this endorsement it is unclear whether the duty to protect is a due diligence requirement under the harm prevention rule, a due diligence requirement under human rights law, or an autonomous distinct duty to protect.[459]

1.1 Spill-over effects of cyber harm to critical infrastructure

Protecting own critical infrastructure against cyber harm is in the self-interest of states. However, cyber operations against critical infrastructure of one state can have ramifications internationally. The UN GGE Report 2021

454 Buchan, 'Obligation to Prevent' 2016 (n. 88), 441.

455 See above chapter 3.C.II; regarding the negative prohibitive dimension of the harm prevention rule requires states to abstain from impairing critical infrastructure of other states, see above chapter 4.A.I.

456 UN GGE Report 2015, para. 13g: 'States should take appropriate measures to protect their critical infrastructure from ICT threats (…).'

457 UN General Assembly Resolution A/RES/73/27, 5 December 2018, para. 1.7.

458 UN OEWG, Final Report, para 31: 'States should continue to strengthen measures to protect of all critical infrastructure from ICT threats, and increase exchanges on best practices with regard to critical infrastructure protection.'

459 Highlighting that protection of critical infrastructure from cyber threats is both in the interests of individuals on the territory as well as of other states due to spillover effects Gross, 'Cyber Responsibility' 2015 (n. 196), 493.

highlighted potential spill-over effects of cyber harm to critical infrastructure:

> '(…) ICT activity that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public can have cascading domestic, regional and global effects.'[460]

Also the UN GGE Report 2015 already recognized that impairment of critical infrastructure vulnerabilities may transcend national borders.[461] The potential transboundary dimension of impairment of critical infrastructure operation is also acknowledged in the EC Directive 2008/114 which introduces the category 'European Critical Infrastructure'.[462] Reflecting this international dimension of critical infrastructure protection, the Netherlands underlined that the adequate protection of critical infrastructure in one state benefits the international community[463], hereby e.g. concurring with *Gross*.[464]

It is hence clear that in many cases cyber harm to the critical infrastructure of one state may also affect the legally protected interests of other

460 UN GGE, Report 2021, para. 42.

461 UN GGE Report 2015, para. 16 d; also the ILA, 'Cybersecurity and Terrorism' 2016 (n. 65), para. 244; Tyson Macaulay, 'The Danger of Critical Infrastructure Interdependency', *Center for International Governance Innovation,* 2019, available at: https://www.cigionline.org/articles/danger-critical-infrastructure-interdependency/.

462 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Rc. 7: 'There are a certain number of critical infrastructures in the Community, the disruption or destruction of which would have significant cross-border impacts. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructures.'

463 Netherlands' response 2020 (n. 30), para. 28: '(…) to address the development that critical infrastructure is no longer confined to the borders of States alone the report should acknowledge that critical infrastructure is increasingly becoming transnational and interdependent and that adequate protection of these critical infrastructures would benefit the international community.'

464 Gross, 'Cyber Responsibility' 2015 (n. 196), 493: 'In a digitally interconnected world, the strength of the digital chain may be only as strong as its weakest link. Cybersecurity incidents that compromise the security or the functionality of a network component in one country may have critical spillover impacts on the security or functionality of other parts of the network, or other networks that are connected or otherwise related to it, and that may directly or indirectly affect other states or non-state actors.

states. Yet, the degree to which interests of other states and the international community are affected by cyber operations against critical infrastructure diverges. For example, in the financial sector the interdependency is likely high: Disruptions of the stock market of one country may affect the stock market and financial services in other states. Disabling the national transport infrastructure, e.g. the national railway, via ransomware may also have spill over effects on other countries. Also impairment of the energy and transport sector is likely to affect the interests of other states.[465] But it cannot be presumed that any impairment of critical infrastructure *per se* affects the rights of other states. If e.g. a cyber operation disrupts the telecommunications services in the region of one state or if local transportation in only one particular city is impaired, a sufficient cross-border would likely lack. It seems hence reasonable to limit a due diligence duty to protect own critical infrastructure to the list of internationally recognized key critical infrastructures.[466] States may individually choose to designate further institutions as critical infrastructure but in such cases the interests of other states are likely not implicated.

1.2 Duty to protect critical infrastructure under human rights law

The duty to protect *own* critical infrastructure may furthermore be required under human rights law. Attacks on critical infrastructure can have severe harmful impacts on individuals. Operations against medical facilities or nuclear reactors may for example interfere with the right to life and the right to health.[467] In September 2020 a woman died after her medical treatment was interrupted by a cyber operation.[468] The exposure of individuals to potentially deadly cyber operations, e.g. against smart vehicles, is likely to

465 Council Directive 2008/114 (n. 462) establishes a procedure for identifying and designating European Critical Infrastructures (ECIs) in the transport and energy sectors whose disruption would have significant cross-border impacts.

466 On key critical infrastructure see chapter 3.C.II.2.3.

467 Depicting impediment of medical treatment Germany following a ransomware attack against a hospital in Neuss, Germany, Bundesamt für Sicherheit in der Informationstechnik (BSI), *Schutz Kritischer Infrastrukturen* (2016), p. 6.

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

increase with the Internet of Things.[469] But cyber harm can also constitute a risk to economic and social rights. In July 2021, a ransomware operation crippled various agencies' capability to pay unemployment and parental aid in a region in Germany[470], leaving affected individuals without potentially vital financial support. Also the harmful consequences for individual of attacks against the financial system have been highlighted.[471] Hence, it is clear that cyber harm against critical infrastructure which constitute a risk to human rights also triggers due diligence duties to protect.[472]

1.3 Best practice standards for protecting critical infrastructure

Para. 13 lit. g of the UN GGE Report 2015 calls on states to exercise 'appropriate measures' to protect their critical infrastructure.[473] Which specific measures states are expected to take is not spelled out but a variety of best practice standards or recommendations exist. E.g. both the UN General Assembly Res. 58/199 of 2004 and the UN General Assembly Res. 64/211 of 2010 provide a 'voluntary self-assessment tool for national efforts to protect critical information infrastructure'.[474] Also the ITU has provided a ITU National Cybersecurity/Critical information infrastructure protection Self-Assessment Tool[475] and the OSCE has addressed critical infrastructure

469 Bannelier/Christakis, 'Prevention Reactions' 2017 (n. 151), 62.

470 Meike Laaff, 'Wie eine Cyberattacke einen ganzen Landkreis lahmlegt', *ZEITOnline*, 12 July 2021, available at: https://www.zeit.de/digital/datenschutz/2021-07/hackeran griff-anhalt-bitterfeld-cyber-katastrophenfall-kommunen-internetkriminalitaet.

471 US Department of Justice, 'Manhattan U.S. Attorney Announces Charges against Seven Iranians for Conducting Coordinated Campaign of Cyber Attacks against U.S. Financial Sector on Behalf of Islamic Revolutionary Guard Corps-Sponsored Entities', Press Release 24 Mach 2016: 'The charges announced today respond directly to a cyber-assault (…) The alleged onslaught of cyber-attacks on 46 of our largest financial institutions (…) resulted in hundreds of thousands of customers being unable to access their accounts (…)'.

472 ILA, 'Cybersecurity and Terrorism' 2016 (n. 65), para. 244.

473 UN GGE Report 2015, para. 13g; UN General Assembly Resolution A/RES/73/27, 11 December 2018, para. 1.7.

474 UN General Assembly Resolution A/RES/58/199, 23 December 2003, Annex Elements for protecting critical information infrastructures; UN General Assembly Resolution A/RES/64/211, Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, 21 December 2009, Annex, p. 3–5.

475 ITU National Cybersecurity/CIIP Self-Assessment Tool, Draft April 2009.

protection measures as CBMs.[476] On the national level, various policies for critical infrastructure protection exist, e.g. in the US the 'Framework for Improving Critical Infrastructure Cybersecurity'.[477] Several of the suggested measures in these guidelines and implemented measures in state practice are worth pointing out.

1.3.1 Ensuring IT security standards

Laws in several countries, e.g. in the EU[478] or China[479], require that critical infrastructure operators meet IT security standards and employ the 'state of the art'.[480] The ITU recommends that states ensure that critical infrastructure operators meet internationally recognized minimum cybersecurity standards[481], a suggestion also reiterated by Canada which referred to 'minimum baseline requirements'.[482] States are well advised to focus on what they consider the minimum requirement of critical infrastructure, e.g. via reference to technical standards, such as ISO, with due consideration of capacity limits of developing countries. One method of raising cyber

476 OSCE, Permanent Council Decision No. 1202, PC.DEC/1202, 10 March 2016, paras. 12–16; OSCE, Permanent Council Decision PC.DEC/1106, 3 December 2013, paras. 1–11.

477 NIST, 'Framework for Improving Critical Infrastructure Cybersecurity 1.1', available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

478 EU, NIS 2 Directive (n. 275), art. 21 (1): 'Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures (…) Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures (…) shall ensure a level of security of network and information systems appropriate to the risks posed (…).

479 Cybersecurity Law of the People's Republic of China, 1 June 2017, art. 23: 'Critical network equipment and specialized cybersecurity products shall follow national standards and mandatory requirements, and be security certified by a qualified establishment or meet the requirements of a security inspection, before being sold or provided (…).'

480 Highlighting the importance of harmonizing technical standards of critical infrastructure Michael Berk, 'Recommendation 13g and h', in Enekken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology – A Commentary* (United Nations Office for Disarmament Affairs 2017), 191–222, at 205.

481 ITU, 'Guide National Cybersecurity Strategy' 2018 (n. 452), p. 43.

482 UN OEWG Chairs Summary 2021 (n. 273), Annex, Canada, p. 13.

security standards may be certification.[483] An important area of adhering to security standards is emergency preparedness.[484]

1.3.2 Criminal legislation

The UN General Assembly[485], the AU Malabo Procotol[486], as well as commentators have underlined that enacting cybercrime legislation is an important tool for protecting one's critical infrastructure.[487] A UN Study in 2013 found that the character of an ICT system attacked as critical infrastructure is an aggravating circumstance in a large number of countries[488], leading to higher penalties. As critical infrastructure is regularly threatened by cyber operations that constitute data or system interference – which states are required to criminalize due to due diligence[489] – due diligence for critical infrastructure protection converges with the due diligence requirement to criminalize.

1.3.3 Inter-state and public-private cooperation

The UN OEWG Final Report broadly referred to the need for cooperation in the context of protection of critical infrastructure[490], similar to France which called for cooperation against risks to critical infrastructure[491] and China which called for exchanges on emergency coordination regarding threats to critical infrastructure.[492] Also the UN Security Council highligh-

483 China, 'Cybersecurity Law' 2017 (n. 481), art. 23; highlighting that certification of critical infrastructure is critical EU, 'Cybersecurity Act' 2019 (n. 261), rc. 65.
484 ILA, 'Cybersecurity and Terrorism' 2016 (n. 65), para. 247.
485 UN General Assembly Resolution A/RES/64/211, 21 December 2009, para. 13–16.
486 Malabo Convention (n. 328), art 25 (4).
487 David P. Fidler, 'Whither the Web?: International Law, Cybersecurity, and Critical Infrastructure Protection', *Articles by Maurer Faculty* 2452 (2015), at 2456; ILA, 'Cybersecurity and Terrorism' 2016 (n. 65), para. 269.
488 UN ODC, 'Comprehensive Study' 2013 (n. 214), p. 85.
489 See above chapter 4.D.I.4.2.
490 UN OEWG Final Report 2021, para. 59: 'Capacity-building aimed at enabling States to identify and protect national critical infrastructure and to cooperatively safeguard critical information infrastructure was deemed to be of particular importance.'
491 France, Stratégie internationale de la France pour le numérique, 2017, p. 32.
492 China, Cyber Attacks Against Critical Infrastructure' (n. 8); see also Foreign Ministry Spokesperson Geng Shuang's Regular Press Conference on April 24, 2020:

ted the need for inter-state cooperation against cyber operations.[493] The substance of such cooperation for critical infrastructure in cyberspace remains undefined but it is to be assumed that at least the procedural due diligence requirements – all of which are underpinned by the normative aspiration of cooperation[494] – also apply with regard to critical infrastructure.

Lastly, as private actors operate the large majority of critical infrastructure, cooperation between private and public actors, e.g. through notification obligations on private actors, as well as regulation of the private sector[495], is crucial for effectively protecting a state's own critical infrastructure.

1.4 Non-binding best practice standards

Commentators have labelled these measures the soft law of critical infrastructure protection.[496] They are hence not binding due diligence requirements but rather best practices for discharging the due diligence obligation to protect *own* critical infrastructure. In particular, establishing minimum security standards for critical infrastructure seems crucial for reducing cyber insecurity. While limited technological capacity will pose a challenge for some states the argument that an objective minimum standard of IT security with regard to critical infrastructure is emerging is particularly strong.

'States should increase exchanges on standards and best practices with regard to critical infrastructure protection, and explore the possibilities to establish relevant risk early warning and information sharing mechanism [and] to improve protection capability for cyber security of states (…).'

493 UN Security Council, S/RES/2341, 13 February 2017, para. 1: Encourages all States to make concerted and coordinated efforts, including through international cooperation, to raise awareness, to expand knowledge and understanding of the challenges posed by terrorist attacks, in order to improve preparedness for such attacks against critical infrastructure.

494 See chapter above 4.C.I.

495 UN GGE Report 2021, para. 49; India, Latest Edits to Zero Draft, 2021, para. 21.

496 Fidler, 'Wither the Web' 2015 (n. 487), 2465; on the soft law character of state practice regarding protection of critical infrastructure ILA, 'Cybersecurity and Terrorism' 2016 (n. 65), para. 243.

2. Duty to prevent cyber harm to the critical infrastructure of other states

For the sake of comprehensiveness, it is to be noted that due diligence requires not only to protect own critical infrastructure but also to take reasonable and appropriate measures to prevent cyber harm to the critical infrastructure of other states. This clarification is due to the fact that even states which have asserted a negative obligation not to damage other state's critical infrastructure, such as China, have notably fallen short of asserting a duty to prevent malicious acts against the critical infrastructure of other states.[497] Only Iran has expressly acknowledged a duty to prevent harm to the critical infrastructure of other states.[498] Overall, states avoid explicit commitments to prevent cyber harm to the critical infrastructure of other states. Yet, there is no teleological reason why preventive due diligence requirements and in particular procedural due diligence obligations should not apply to cyber operations against critical infrastructure of other states. Cyber harm to critical infrastructure is consistently highlighted by states as particularly harmful.[499] Also para. 13 lit. h of the UN GGE Report 2015 requires states to 'respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts'[500], indicating that states recognize their responsibility to mitigate cyber risk to the critical infrastructure of other states. Also the assertion by China which highlighted the importance of early warning regarding cyber risks to critical infrastructure[501] further underscores the acknowledgment of the necessity to mitigate transboundary risks to critical infrastructure. States are well advised to distinguish and commit more clearly between preventive obligations and best practices for the protection of their *own* critical infrastructure and the duties to prevent harm to the critical infrastructure of other states.

497 UN OEWG Chairs Summary 2021 (n. 273), Annex, China, p. 15.

498 Iran, Zero draft report of the Open-ended working group On developments in the field of information and telecommunications in the context of international security, UN OEWG, January 2021, p. 13: 'All forms of interventions and interference or attempted threat against (…) cyber related critical infrastructure of the states shall be condemned and prevented'.

499 See chapter 3.C.III.

500 UN GGE Report 2015, para. 13h.

501 China, Foreign Ministry, 'Press Conference' 2020 (n. 492): 'States should (…) explore the possibilities to establish relevant risk early warning and information sharing mechanism (…) in case of cyber attacks against critical infrastructure.'

IV. The establishment of computer emergency response teams and points of contact for international cooperation

In the international legal discourse both CERTs, as well as national points of contact are frequently mentioned in discussions on the UN level, e.g. in the UN GGE[502] or UN OEWG reports[503], or in individual statements of states.[504] Also commentators have acknowledged the importance of CERTs.[505] This raises the question whether due diligence for harm prevention requires the establishment of both CERTs, as well as generally the establishment of national points of contact.

1. Divergent understandings of emergency response teams and points of contact

CERTs are institutions for incident response and mitigation in emergencies.[506] The UN GGE Report 2021 circumscribed CERTs as

> 'essential to effectively detecting and mitigating the immediate and long-term negative effects of ICT incidents'[507]

The definition of 'points of contact' partially overlaps with the CERT. First, CERTs are international point of contact during cyber incidents, as

502 UN GGE Report 2021, para. 21; UN GGE Report 2015, para. 13k.
503 UN OEWG, Pre-Draft Report 2020, para. 44.
504 Cuba, Considerations on the Initial Pre-Draft of the Open-Ended Working Group, 2020, p. 3; Canada's implementation of the 2015 GGE norms 2019 (n. 166), p. 13.
505 Woltag, 'Cyber Warfare' 2014 (n. 212), 69.
506 Schmitt, 'Tallinn Manual 2.0' 2017 (n. 14), Glossary, p. 563: 'A team that provides initial emergency response aid and triage services to the victims or potential victims of 'cyber operations' (see below) or cyber crimes, usually in a manner that involves coordination between private sector and government entities'; Roy Schondorf, Israel Ministry of Justice, Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations, 8 December 2020: 'CERTs are already doing what could arguably fall into th[e category of due diligence][addition by the author]: exchanging information with one another, as well as cooperating with each other in mitigating incidents'. CERTs as 'authorized emergency response teams', see UN GGE Report 2015, para. 13k.
507 UN GGE Report 2021, para. 65.

highlighted by states[508] or in cybercrime treaties.[509] Second, further 'points of contact' beyond CERTs exist, such as contact points for 'diplomatic, policy, legal and technical exchanges'[510], or for information exchange and assistance in investigations.[511] The notion of points of contact is hence amorphous and not to be understood as a technical legal term but rather – in the very meaning of the word – as context-dependent points of contact. It is hence necessary to take the context and a certain degree of ambiguity into account when assessing references to CERTs and points of contact in international legal practice.

2. Establishment of CERTs and points of contact as a due diligence requirement

Establishing a national CERT as a capacity-building measure could be considered a due diligence measure envisioned by Art. 16 of the ILC Draft Prevention Articles which requires emergency preparedness (i.e. contingency plans to respond to incidents).[512] It could also be grasped under Art. 5 of the Draft Prevention Articles which requires the establishment of the necessary legislative, administrative or other action.[513]

States and commentators have highlighted the importance of establishing a CERT or a national point of contact for cyber risk mitigation and have also linked it to due diligence. South Korea for example suggested that designation of a national point of contact by the UN OEWG would be worthwhile to discharge due diligence.[514] Israel similarly referred to CERTs

508 Australia, 'Cyber Engagement Strategy' 2017 (n. 149), p. 25; New Zealand, Cyber security strategy 2016, Action Plan Annual Report, p. 2: 'CERT NZ will be the international point of contact for cyber security matters, working closely with CERTs in other countries to prevent and respond to cyber security incidents'.

509 Convention on Cybercrime 2001 (n. 215), art. 35.

510 UN OEWG Final Report, para. 47.

511 UN GGE Report, para. 17b.

512 ILC Draft Articles on Prevention 2001 (n. 31), art. 16: 'The State of origin shall develop contingency plans for responding to emergencies, in cooperation, where appropriate, with the State likely to be affected and competent international organizations.'

513 Ibid., art. 5: 'States concerned shall take the necessary legislative, administrative or other action including the establishment of suitable monitoring mechanisms to implement the provisions of the present articles.'

514 Republic of Korea, 'Comments' 2020 (n. 30), p. 5.

in the context of due diligence.[515] Also Guatemala has asserted that states are required to establish a CERT.[516] Ecuador has asserted that establishment of CERTs is crucial for identifying harmful activities and directly linked such establishment to due diligence in cyberspace.[517] The UN OEWG Final Report reiterates that a national point of contact is 'invaluable' and helpful for other CBMs.[518]

The UK referred to its designation of a national point of contact with regard to its implementation of the para. 13 UN GGE 2015 norms.[519] Already in 2008, the Arab states discussed that countries should establish a CERT for incident response.[520] Regarding alleged ransomware operations emanating from Russian soil US president Biden underlined the setting up of communication channel as instrumental for effective ransomware prevention

> 'United States expects when a ransomware operation is coming from [Russia's] soil – even though it's not sponsored by the state – we expect [Russia] to act (…) We've set up a means of communications now, on a regular basis, to be able to communicate to one another when each of us thinks something's happening in the other country.'[521]

Commentators have also pointed out that a point of contact is necessary for exchanges about vulnerabilities and remedies.[522]

There is hence overall strong evidence of increasing state practice and opinio iuris which affirms the importance of CERTs for risk mitigation and prevention in cyberspace, inter alia through procedural due diligence

---

515 Schondorf, 'Israel's Perspective' 2020 (n. 506).

516 Organization of American States, Improving Transparency — International Law and State Cyber Operations: Fourth Report (Presented by Prof. Duncan B. Hollis), CJI/doc. 603/20 rev.1 corr.1, 5 March 2020, p. 20, para. 58.

517 Ecuador, 'Preliminary comments' 2020 (n. 192), p. 2.

518 UN OEWG Final Report, para. 47.

519 UK, 'Efforts to Implement Norms' 2019 (n. 87), p. 15.

520 ITU, 'Arab States call for heightened cybersecurity', Press Release on Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection on 18–21 February 2008 in Doha: 'Participants called for each country to create a national focal point for monitoring and responding to breaches in cybersecurity. Typically, this would take the form of a national computer security incident response team (CSIRT)'.

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

522 Tsagourias, 'Recommendation 13j' 2017 (n. 200), para. 38.

obligations. Non-state actors such as Microsoft, as well as the UN GGE Reports, have asserted that CERTs may even be designated national critical infrastructure.[523]

3. Establishment of CERTs and points of contact under binding and non-binding norms

The establishment of CERTs is also required under binding regional treaty law. Art. 35 of the Budapest Convention requires states to establish national points of contacts for immediate assistance and evidence collection.[524] The establishment of a national CERT is also required under art. 10 (1) of the NIS 2 Directive of the EU.[525] In state practice, networks of points of contact for cybercrime prosecution exist.[526] Such national points of contact are available on a 24/7 basis and provide immediate assistance in case of emergencies. Points of contacts for cybercrime cooperation hence resemble the function of CERTs mentioned at the UN level as responsible point of contact in emergencies.[527] The Draft Report of the Expert Group Cybercrime of 2020 notably urged states to 'strengthen networks of collaboration among CERTs', hereby suggesting the equivalence of CERTs and points of contact for cybercrime cooperation. States may hence consider to designate one institution as both a CERT envisioned in the UN GGE and point of contact stipulated by cybercrime treaties.

Despite the often indeterminate references in international legal practice this state practice highlights that the establishment of CERTs or national point of contact regarding cyber incidents is already largely presupposed by states. States are so far cautious to commit to establishing CERTs as legally

523 Microsoft, Protecting People in Cyberspace: The Vital Role of the United Nations in 2020, 4 December 2019, p. 4.

524 Convention on Cybercrime 2001 (n. 215), art. 35: 'Each Party shall designate a point of contact available on a twenty-four hour, seven-daya-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence (…)'.

525 EU, NIS 2 Directive (n. 275), art. 10 (1).

526 Highlighting their relevance for international cooperation Report Expert Group 2019 (n. 253), para. 10h.

527 Stipulating the point of contact under Art. 35 of the Budapest Convention as potential contact in case of emergencies Cybercrime Convention Committee (T-CY), Draft AP II, 2018 (n. 145), para. 8, p. 5.

binding obligation. References to CERTs are frequently made in legally ambiguous terms, e.g. as CBMs, in the UN GGE[528] or individual statements by states.[529] Also the Final Report of the UN OEWG explicitly asserted that establishment of a national points of contact as a CBM.[530] Yet, the persistent assumption of the existence of such CERTs as points of contacts[531], as well as their instrumentality for discharging other potential diligence obligations[532], such as e.g. to assist with regard to ongoing incidents, or to warn or to cooperate in cybercrime investigations strongly suggests to consider the establishment of CERT a binding due diligence requirement.[533] The reluctance of states may inter alia be due to uncertainty about the functions and responsibilities of such institutions. A global repository, as envisaged by the Netherlands[534], the Philippines[535] may further clarity in this regard.[536]

For the sake of comprehensiveness, it is to be noted that states are obliged not to cause harm or to prevent harm to the CERTs of *other* states. The negative prohibition is explicitly asserted in para. 13 lit. k of the UN GGE Report.[537]

528 UN GGE Report 2013, para. 26 lit. d; UN GGE Report 2015, para. 17c; UN GGE Report 2021, para. 76.
529 Netherlands' response 2020 (n. 30), paras. 33–36.
530 UN OEWG Final Report 2021, para. 47.
531 See e.g. African Union, Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, 29 January 2024 (endorsed by the Assembly of the AU on 18 February 2024), paras. 25, 66.
532 UN GGE Report 2021, para 27: 'Cooperation at the regional and international levels, including between national Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs), the ICT authorities of States and the diplomatic community, can strengthen the ability of States to detect and investigate malicious ICT incidents and to substantiate their concerns and findings before reaching a conclusion on an incident.' UN OEWG, Final Report 2021, para. 47: 'As a specific measure, States concluded that establishing national Points of Contact (PoCs) is a CBM in itself, but is also a helpful measure for the implementation of many other CBMs, and is invaluable in times of crisis. States may find it useful to have PoCs for, inter alia, diplomatic, policy, legal and technical exchanges, as well as incident reporting and response'.
533 Woltag, 'Cyber Warfare' 2014 (n. 212), 106.
534 Netherlands' response 2020 (n. 30), para. 35.
535 Philippine Intervention on the Zero Draft, p. 1.
536 UN OEWG Chairs Summary 2021 (n. 273), para. 31.
537 See above chapter 4.A.II.

V. Evolving due diligence standard regarding institutional capacity

The preceding analysis has shown that due diligence requires a number of institutional safeguard measures as the organisational minimum standard. States cannot claim that they acted diligent if they have not enacted cybercrime legislation on key cybercrime offences or if they have not to established central cyber investigative measures. States are furthermore obliged to use existing channels of acquiring knowledge and also to establish certain basic channels of knowledge, e.g. via establishing reporting obligations on non-state actors. Furthermore, due diligence requires that states protect their *own* critical infrastructure, both under the harm prevention rule, as well as international human rights law. Due diligence for harm prevention also requires states to establish CERTs as points of contact in case of international cyber incidents, as well as points of contact for cybercrime cooperation. To relegate such measures to the level of non-binding guidelines[538] would not do justice to the indispensable function of such measures for fostering cyber resilience.

It is however to be cautioned that the required due diligence standard is not uniform and that states have discretion in implementing the precise requirements. Hence, with regard to all of the above-mentioned measures due diligence allows for divergences. With regard to the criminalization of states may e.g. choose to introduce *de minimis* requirements, criminalization exemptions for legitimate acts or additional criminalization requirements. With regard to cyber investigative measures states' divergences in technological capacity may soften the required standard. In establishing investigative capabilities states are required to install human rights safeguards. Regarding the required level of monitoring of cyber activities in a state's territory states are required to use the existing means of acquiring knowledge and, as a bottomline, to keep being informed about cyber activities in their territory. Ensuring appropriate IT security standards in critical infrastructure may be an emerging minimum standard of protecting one's own critical infrastructure but beyond this other protective measures can only be considered the 'soft law' of critical infrastructure protection. With regard to the establishment of CERTs and international points of contact

538 On criminalization of malicious cyber activities as a mere 'guideline' but not a binding requirement see Coco/Dias, 'Cyber Due Diligence Report' 2021 (n. 129), 202, 206.

the precise mode of establishment, function and responsibilities remains within a state's discretion.

Beyond these institutional capacity-building measures it is clear that in order to effectively discharge address risks of cyber harm states need to comprehensively and holistically address cyber security risks, e.g. via reassessing legislation including regulatory and liability regimes for network operators, telecommunication companies, or encryption services, or data security. To this aim, states have regularly adopted comprehensive cyber security strategies.[539] It is clear that at a minimum such strategies should systematically assess cyber risks. As an international standard for cybersecurity strategies can however not meaningfully be approximated, it cannot be considered a due diligence requirement.

539 See in more detail states' national strategies Coco/Dias, 'Cyber Due Diligence Report' 2021 (n. 129), 216, 217.