The European Journal of International Law Vol. 32 no. 3

'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law

Antonio Coco[*] and Talita de Souza Dias[**]

Abstract

With a long history in international law, the concept of due diligence has recently gained traction in the cyber context, as a promising avenue to hold states accountable for harmful cyber operations originating from, or transiting through, their territory, in the absence of attribution. Nonetheless, confusion surrounds the nature, content and scope of due diligence. It remains unclear whether it is a general principle of international law, a self-standing obligation or a standard of conduct, and whether there is a specific rule requiring diligent behaviour in cyberspace. This has created an 'all-or-nothing' discourse: either states have agreed to a rule or principle of 'cyber due diligence', or no obligation to behave diligently would exist in cyberspace. We propose to shift the debate from label to substance, asking whether states have duties to protect other states and individuals from cyber harms. By revisiting traditional cases, as well as surveying recent state practice, we contend that – whether or not there is consensus on 'cyber due diligence' – a patchwork of different protective obligations already applies, by default, in cyberspace. At their core is a flexible standard of diligent behaviour requiring states to take reasonable steps to prevent, halt and/or redress a range of online harms.

1 Introduction

Due diligence has recently become a buzzword in the 'cyber domain'. The renewed interest in the concept can be explained by the persistent challenges of factually and legally attributing malicious cyber operations to states. Anonymizing and rerouting techniques,

[*] Lecturer, School of Law, University of Essex, Colchester, United Kingdom. Email: antonio.coco@essex.ac.uk.
[**] Shaw Foundation Junior Research Fellow in Law, Jesus College, University of Oxford, Oxford, United Kingdom. Email: talita.desouzadias@jesus.ox.ac.uk.
The research for this article was funded by the Government of Japan. The views expressed in the article, however, do not necessarily reflect those of the funder. Among others, we would like to thank Dapo Akande, Tomohiro Mikanagi and Przemysław Roguski for their helpful comments on earlier drafts. Any error remains, of course, our own.

such as virtual private networks (VPNs) and other internet protocol (IP) spoofing software, have compounded the attribution problem.[1] In this context of great uncertainty and increased cyber threats, due diligence features as a promising route to accountability, peace and security in cyberspace: it requires states to employ their best efforts to prevent, halt and redress a range of known or foreseeable cyber harms emanating from or transiting through their territory, regardless of who or what caused them. For instance, during the COVID-19 pandemic, EU member states have 'call[ed] upon every country to exercise due diligence and take appropriate actions against actors conducting [malicious cyber operations] from its territory, consistent with international law'.[2]

Yet controversy remains as to whether states are bound by an obligation to behave diligently in cyberspace, an area of state activity that comprises information and communication technologies (ICTs) having a physical, logical and personal dimension.[3] On the one hand, the 2015 report by the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (hereinafter 'GGE'), adopted by consensus by the UN General Assembly,[4] indicates that states '*should* not knowingly allow their territory to be used for internationally wrongful acts using ICTs'.[5] The provision is explicitly framed as a

1 Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', 21 *Journal of Conflict & Security Law* (*JCSL*) (2016) 429, at 432.

2 Council of the European Union, Press Release, 'Declaration by the High Representative Josep Borrell, on Behalf of the European Union, on Malicious Cyber Activities Exploiting the Coronavirus Pandemic' (30 April 2020), available at www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/. A similar statement was made by the European Union and endorsed by member states during the UN Security Council Arria-Formula Meeting on Cyber Stability and Conflict Prevention and Capacity Building: see Pawel Herczynski, Statement on behalf of the European Union (20 May 2020), at 2, available at https://vm.ee/sites/default/files/Estonia_for_UN/20_05_22_arria_cyber_eu_statement_as_delivered_unread_paras.pdf. See also, e.g., Mona Juul, Ambassador, Joint statement from Denmark, Finland, Iceland, Sweden and Norway at the Arria-Meeting on Cyber Stability and Conflict Prevention (22 May 2020), available at www.norway.no/en/missions/UN/statements/security-council/2020/arria-cyber-stability-and-conflict-prevention. Along the same lines, but without explicitly mentioning due diligence, see Republic of Poland, Statement by H.E. Tadeusz Chomicki Ambassador for Cyber & Tech Affairs Ministry of Foreign Affairs (2020), at 1, available at https://vm.ee/sites/default/files/Estonia_for_UN/statement_of_poland_arria_un_sc_on_cyber_22.05.2020.pdf; Italy's Statement at the Arria Formula Meeting on Cyber Stability, Conflict Prevention and Capacity Building (2020), at 1, available at https://vm.ee/sites/default/files/Estonia_for_UN/riunione_del_cds_in_formato_arria.pdf. It is also worth noting that over 130 scholars and practitioners acting in their individual capacity accepted that states *already* have obligations to prevent malicious cyber operations emanating from their territory or jurisdiction against the healthcare sector, especially during the COVID-19 outbreak: see The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector, available at https://elac.web.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea (last visited 10 July 2021).

3 Sullivan, 'The 2014 Sony Hack and the Role of International Law', 8 *Journal of National Security Law and Policy* (2015) 437, at 454 n.88. See also Tsagourias, 'The Legal Status of Cyberspace', in N. Tsagourias and R. Buchan (eds), *Research Handbook on International Law and Cyberspace* (2015) 13; Johnson and Post, 'Law and Borders: The Rise of Law in Cyberspace', 48 *Stanford Law Review* (1996) 1367.

4 GA Res. 70/237, 30 December 2015, §§ 1–2(a).

5 Report of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174, 22 July 2015, § 13(c) ('UN GGE Report 2015') (emphasis added).

'voluntary, non-binding norm' of responsible state behaviour in cyberspace. On the other hand, the group of experts involved in the second edition of the *Tallinn Manual on the International Law Applicable to Cyber Operations* (hereinafter 'the Tallinn Manual') agreed that a general rule or principle of this kind already exists in customary international law, and is applicable in cyberspace.[6] Rule 6 of the Tallinn Manual requires a state to 'exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other states'.[7] On their face, these views seem irreconcilable, and neither of them has gone unchallenged.[8]

We contend that the current debate misses the point by focusing too much on the meaning of 'due diligence' and its applicability to cyberspace. This has resulted in binary, 'all-or-nothing' views: either consensus has been reached on what is 'cyber due diligence' or there would be a legal gap in protection – states would have no binding obligations but only voluntary undertakings to behave diligently in their use of ICTs. The confusion partly stems from the inconsistent use of the label 'due diligence' as a general principle of law or international law, one or more state obligations or a standard of behaviour applying in different areas of international law.[9]

6 M. Schmitt (ed.), *Tallinn Manual 2.0* (2nd ed. 2017) 30, rule 6; 43, rule 7 (hereinafter *Tallinn Manual 2.0*).

7 *Ibid.*, at 30. The Manual is the result of the work of a group of experts and seeks to comprehensively analyse how international law applies in cyberspace.

8 For instance, Jensen and Watts are cautious about the legal basis of this rule, recognizing its advantages but also warning about its drawbacks. See Jensen and Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?', 95 *Texas Law Review* (2017) 1555, at 1568–1575. With respect to the supposed burden that the GGE recommendation would impose on states, making them wary to accept it, see L. Adamson, 'Recommendation 13(c)', in United Nations Office of Disarmament Affairs, *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary* (2017) 49, at 55, § 12. At least four states (Argentina, Israel, New Zealand and the United Kingdom) have expressed scepticism about the rule: see Argentina, Statement at the 2nd substantive session of the open-ended working group on developments in the field of information and telecommunications in the context of international security (hereinafter 'OEWG') (11 February 2020), available at https://media.un.org/en/asset/k18/k18w6jq6eg (timestamp 02:15:05, hereinafter 'Argentina's OEWG Statement'); Schondorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations', *EJIL: Talk!* (9 December 2020), available at www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/; and, albeit in a less clear-cut way, New Zealand, The Application of International Law to State Activity in Cyberspace (1 December 2020), § 17, available at https://dpmc.govt.nz/publications/application-international-law-state-activity-cyberspace; United Kingdom Mission to the United Nations, United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security: Application of International Law to States' Conduct In Cyberspace (3 June 2021), available at https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement, para 10.

9 See McDonald, 'The Role of Due Diligence in International Law', 68 *International and Comparative Quarterly* (*ICLQ*) (2019) 1041, at 1043–1044 n.13; Koivurova, 'Due Diligence', in *Max Planck Encyclopaedia of Public International Law* (MPEPIL) (2010), paras 1–2, available at opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1034?prd=EPIL (referring to due diligence as 'an obligation of conduct' as well as a 'concept' and a 'general principle of law').

To avoid those confusions and contradictions, we propose to shift the debate from label to substance. Rather than inquiring whether 'due diligence' applies in cyberspace, the question we should be asking is to what extent states have obligations to protect other states and individuals from cyber harms. In answering this question, we conclude that whether or not a general principle of due diligence applies to ICTs or a binding, cyber-specific 'due diligence rule' exists, states continue to be bound by a patchwork of duties to prevent, stop and redress harm applying by default to cyberspace. These 'protective obligations' are grounded in several primary rules of international law enshrining a standard of due diligence – that is, obligations that require states to exert their best efforts in preventing, halting and redressing a variety of harms, online and offline.

This article begins, in Section 2, by explaining why, despite the longstanding confusion surrounding its exact meaning and scope, we believe that 'due diligence' in international law is better understood as a standard of conduct. This standard usually refers to harm prevention, mitigation and redress, but it varies across the different 'protective' obligations where it is found, as well as the states, circumstances and fields in which they apply. Examples include international environmental law, law of the sea, diplomatic protection, international investment law, international humanitarian law and international human rights law, under treaty or customary international law.[10]

Section 3 then explains why the entirety of international law – including the said 'protective' obligations – applies by default to cyberspace, in the absence of a rule to the contrary. This claim is backed by evidence of relevant state practice and expressions of *opinio juris*.

In what is this article's main contribution to the current academic debate, Section 4 maps out four sets of protective duties requiring states to prevent, halt or redress certain harms by behaving diligently in cyberspace. Two of these can be traced to primary obligations of general international law: (i) the duty of states not to knowingly allow their territory to be used for acts that are contrary to the rights of third states, articulated in the *Corfu Channel* case,[11] which we call the 'Corfu Channel' principle;[12] and (ii) states' duty to prevent and remedy significant transboundary harm, even if caused by lawful activities, known as the 'no-harm' principle.[13] In addition, specific bodies of international law establish due diligence duties which also apply to cyberspace. Of particular relevance to ICTs are: (iii) the obligation of states to protect human rights within their jurisdiction; and (iv) states' duties to ensure respect

[10] Koivurova, *supra* note 9, paras 29–31, 45.

[11] *Corfu Channel* (*United Kingdom v. Albania*), Judgment, 9 April 1949, ICJ Reports (1949) 4, at 22 (hereinafter '*Corfu Channel*').

[12] See Reinisch and Beham, 'Mitigating Risks: Inter-State Due Diligence Obligations in Case of Harmful Cyber-Incidents and Malicious Cyber-Activity – Obligations of the Transit State', 58 *German Yearbook of International Law* (*GYIL*) (2015) 101, at 106 (framing the Corfu Channel principle as a 'conflict-related no harm rule').

[13] See *Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Judgment, 20 April 2010, ICJ Reports (2010) 14, paras 101, 187, 197, 204, 223 (hereinafter '*Pulp Mills*').

for international humanitarian law and to adopt precautionary measures against the effects of attacks in the event of an armed conflict. We locate the legal basis of each of those primary rules in customary or conventional international law, unpack the various standards of due diligence they enshrine and explore the extent to which they apply to states' use of ICTs.

Lastly, Section 5 demonstrates that, despite their multifaceted nature, common features belie different protective obligations. As such, they might apply concurrently and inform one another's interpretation in cyberspace and beyond.

The 'patchwork approach' marks a paradigm shift in the understanding and conceptualization of international law concerning diligent state behaviour in cyberspace. Though not a silver bullet against current cybersecurity challenges, we conclude that this international legal 'patchwork' of protective obligations does provide a solid and comprehensive legal basis for harm prevention and accountability.

2 The Nature and Function of Due Diligence in International Law

Despite the renewed interest in due diligence,[14] the concept is not new. Its modern origins can be traced back to a series of 19th and early 20th century arbitrations relating to the protection of aliens abroad.[15] Already at that time, due diligence was linked to a positive obligation of conduct, a 'best efforts' duty, requiring states to act with reasonable care in the circumstances, and holding them responsible for wilfully negligent omissions. Later on, the *Island of Palmas* arbitral award found that such obligation is a corollary of states' sovereign rights over their territory, requiring them to protect the rights of other states therein.[16] Since then, the concept has evolved alongside several primary rules of international law.

First, in the *Corfu Channel* case, the International Court of Justice (ICJ) held that 'it is every State's obligation not to allow knowingly its territory to be used for *acts contrary to the rights of other States*',[17] most – but not all – of which constitute internationally wrongful acts.[18] This duty, framed as a 'well-recognized principle of international

[14] For general studies on the topic, see, e.g., International Law Association (ILA), Study Group on Due Diligence, 2nd Report (2016), available at www.ila-hq.org/index.php/study-groups labelled as 'Draft Study Group Report Johannesburg 2016.pdf' (hereinafter 'ILA Study'). Koivurova, *supra* note 9; H. Krieger, A. Peters, and L. Kreuzer (eds), *Due Diligence and Structural Change in the International Legal Order* (2020); J. Kulesza, *Due Diligence in International Law* (2016); Pisillo-Mazzeschi, 'The Due Diligence Rule and the Nature of the International Responsibility of States', 35 *GYIL* (1992) 9.

[15] See, e.g., *Alabama Claims (United States v UK)* (1872) 29 RIAA 125, at 127, 129, 131–132; *Wipperman (United States v Venezuela)* (1887), reprinted in J. Bassett Moore, *History and Digest of the International Arbitrations to Which the United States Has Been a Party*, vol. 3 (1898) 3039, at 3041; *Neer (United States v Mexico)* (1926) 4 RIAA 60, at 61–62.

[16] *Island of Palmas (or Miangas) (United States v Netherlands)*, 4 April 1928, II RIAA 829 (1928), ICGJ 392 (PCA 1928), at 839 (hereinafter '*Island of Palmas*').

[17] *Corfu Channel*, Judgment, 9 April 1949, ICJ Reports (1949), at 22 (emphasis added).

[18] See Section 4.A below.

law', applies generally to all states,[19] and a failure to exercise the requisite degree of diligence gives rise to state responsibility.[20]

Second, as a result of the growing concern over environmental harm and other hazards crossing national borders, due diligence also features in the general obligation not to cause significant transboundary harm to persons, property or the environment.[21] This obligation exists at least since 1941, when the *Trail Smelter* arbitral tribunal found that a state 'owes at all times a duty to protect other states against *injurious acts* by individuals from within their jurisdiction'.[22] Likewise, Article 3 of the International Law Commission's (ILC) 2001 Draft Articles on Prevention of Transboundary Harm from Hazardous Activities recognizes a duty of States to 'take all appropriate measures to prevent significant transboundary *harm* or at any event to minimize the risk thereof'.[23] This provision mirrors customary international law,[24] and is, according to the ILC, an 'obligation of due diligence', requiring states not to successfully prevent or halt significant transboundary harm, but 'to exert [their] best possible efforts to minimize [such] risk'.[25] The customary basis of this duty, known as the 'no-harm' or 'good neighbourliness' principle, has also been affirmed by the ICJ,[26] which noted its origins in the broader 'principle of prevention', alongside the Corfu Channel principle.[27]

Similar duties to behave diligently exist under international human rights law (IHRL). These are positive obligations of states to protect and ensure individual human rights, whether online or offline,[28] to the extent possible.[29] Likewise, the duties to ensure respect for international humanitarian law (IHL) and to take precautions to protect civilians against the effects of attacks during armed conflict are also obligations to exercise due diligence.[30] And other more or less specific duties of reasonable care arise in respect of different harms, such as the duty to prevent genocide under Article I of the Genocide Convention,[31] the obligation to prevent marine pollution,[32] the duty to

19 *Corfu Channel*, Judgment, 9 April 1949, ICJ Reports (1949), at 22.

20 See International Law Commission (ILC), Articles on Responsibility of States for Internationally Wrongful Acts, GA Res. 56/83, 12 December 2000, art. 14(3) (hereinafter 'ARSIWA').

21 See ILC, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, in Report of the International Law Commission on the work of its fifty-third session (23 April–1 June and 2 July–10 August 2001), UN Doc. A/56/10, 144, at 148–149 (hereinafter 'Draft Articles on Prevention'). See also Brunée and Meshel, 'Teaching an Old Law New Tricks: International Environmental Law Lessons for Cyberspace Governance', 58 *GYIL* (2015) 129, at 134–135; Koivurova, *supra* note 9, paras 16, 23, 44–45.

22 *Trail Smelter* (*United States v. Canada*) (1941) 3 RIAA 1911, at 1963.

23 ILC, Draft Articles on Prevention, *supra* note 21.

24 Koivurova, *supra* note 9, para. 10.

25 ILC, Draft Articles on Prevention, *supra* note 21, at 154, Commentary to art. 3, para. 7.

26 *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, ICJ Reports (1996) 226, para. 2 (hereinafter '*Nuclear Weapons*').

27 *Pulp Mills*, Judgment, 20 April 2010, ICJ Reports (2010), para. 101.

28 See also United Nations Human Rights Council (HRC), Res. 32/13 ('The promotion, protection and enjoyment of human rights on the Internet'), UN Doc. A/HRC/RES/32/13, 1 July 2016, § 1.

29 See generally Koivurova, *supra* note 9, para. 45.

30 *Ibid.*, para. 31.

31 Convention on the Prevention and Punishment of the Crime of Genocide, 1948, 78 UNTS 277, art. 1 (hereinafter Genocide Convention). See also *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, Judgment, 26 February 2007, ICJ Reports (2007) 43, paras 430–431.

32 UN Convention on the Law of the Sea, 1982, 1833 UNTS 397, art. 194(2) (hereinafter 'UNCLOS').

ensure that mining activities in the deep seabed area do not cause damage to the environment and human life[33] and duties to cooperate in the investigation and prosecution of transnational crime.[34]

This variety of primary rules recognizing a duty of reasonable care suggests that 'due diligence' itself is simply a standard of behaviour that is found in different 'protective' obligations and varies across different fields, duty-bearers and factual circumstances.[35] Thus, references made in the literature to 'due diligence obligations' or 'duties of due diligence' seem to be a shorthand for a series of obligations which have in common the imposition of a preventive or remedial duty, compliance with which is measured against a certain standard of diligent behaviour.[36] Thus, lack of due diligence gives rise to a breach of an international obligation, in the same way that negligence, or lack of reasonable care, entails a breach of a duty of care in many domestic legal systems.[37] As the International Law Association (ILA) found in its recent study on the topic:

> At its heart, due diligence is concerned with supplying *a standard of care against which fault can be assessed*. It is a *standard of reasonableness, of reasonable care*, that seeks to take account of the consequences of wrongful conduct and the extent to which such consequences *could feasibly have been avoided* by the State or international organisation that either commissioned the relevant act or which omitted to prevent its occurrence.[38]

Those various duties primarily seem to involve a triangular relationship between (i) the duty-bearer, i.e. the state having an obligation to behave diligently in preventing, halting or redressing the harm or the risk thereof; (ii) the source of harm, i.e. the state, non-state entity or natural event causing the harm; and (iii) the beneficiary of the duty, i.e. the state or non-state entity suffering the consequences of the harm.[39] It is for this reason that we conceptualize and frame these duties as 'protective obligations', in that they require the duty-bearer to behave diligently in protecting the beneficiary against harm. Possible sources of harm include state agents, private individuals acting alone or in groups, as well as corporations. Beneficiaries, who may or may not hold a specific right vis-à-vis the duty-bearer, could be other states, individuals or private companies.[40] When the duty-bearer state is the very source of the harm affecting an

[33] *Ibid.*, arts 139, 153(4) and Annex III, art. 4(4). See also *Responsibilities and Obligations of States with Respect to Activities in the Area*, Advisory Opinion, 1 February 2011, ITLOS Reports (2011) 10, paras 107–123, 136, 141–142, 147, 189, 217, 219, 239.

[34] See, e.g., International Convention for the Suppression of the Financing of Terrorism, 1999, 2178 UNTS 197, art. 18; United Nations Convention against Transnational Organized Crime, 2000, 2225 UNTS 209, art. 7.

[35] See Krieger and Peters, 'Due Diligence and Structural Change in the International Legal Order', in Krieger, Peters and Kreuzer, *supra* note 14. See also McDonald, *supra* note 9.

[36] See Koivurova, *supra* note 9, paras 8–9.

[37] Kolb, 'Reflections on Due Diligence Duties and Cyberspace', 58 *GYIL* (2015) 113, at 116; Jensen and Watts, *supra* note 8, at 1566; Pisillo-Mazzeschi, *supra* note 14, at 40, 42; *Neer (United States v Mexico)* (1926) 4 RIAA 60, at 61.

[38] ILA Study, *supra* note 14, at 2 (emphasis added). See also Kulesza, *supra* note 14, at 262–270.

[39] Besson, 'Due Diligence and Extraterritorial Human Rights Obligations – Mind the Gap!', 9 *ESIL Reflections* (2020) 2, at 4–5.

[40] *Ibid.*, at 5.

individual or an object, and the relationship with the beneficiary is linear rather than triangular, whether or not the protective duty is one of due diligence depends on the primary obligation in question. The Corfu Channel principle seems to be limited to a duty to prevent third-party activities that cannot be attributed to the duty-bearer state.[41] In contrast, the no-harm principle,[42] duties to protect and ensure human rights[43] and obligations to take precautions under IHL[44] all seem to apply not only to cases where the duty-bearer state fails to prevent harm by third parties but also where the state *itself* causes the harm in question and thereby fails to prevent, stop or redress it.

Thus, protective obligations have been commonly associated with the idea that states must behave diligently with a view to preventing, stopping or redressing a variety of harms or risks to persons, property or territory, ranging from internationally wrongful acts to lawful activities or even accidents. Each primary obligation to exercise due diligence is triggered and limited by a variety of factors, including (i) the existence of a specific *type* of harm or risk; (ii) the crossing of a threshold of *seriousness* of this harm or risk; (iii) a *nexus* between the state and the harm or risk in question; (iv) some degree of *knowledge* of the harm or risk; and (v) a state's *capacity* to act in the circumstances.[45] However, as will become clearer in the following sections, each of those elements might differ across various protective duties.

We contend that these duties, found in different branches of conventional and customary international law, cover numerous aspects, uses and consequences of ICTs, as they do with other technologies. In what follows, we first establish the applicability of some of those duties to ICTs. We then delve deeper into the extent to which these duties require states to prevent, halt and redress online harms.

3 The Applicability of Existing Protective Obligations in Cyberspace

As a preliminary point, the applicability of existing protective obligations to cyberspace might be challenged on two principal legal bases. First, one may query whether

41 Pisillo-Mazzeschi, *supra* note 14, at 31–34, citing *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States)*, Judgment, 27 June 1986, ICJ Reports (1987) 14, para. 157 (finding that the United States was responsible for actively supporting the Contras, thus breaching its duty to abstain from such support, whereas Nicaragua was responsible for tolerating arms traffic, thus breaching its due diligence duty to protect).

42 ILC, Draft Articles on Prevention, *supra* note 21, at 159, Commentary to art. 8, para. 2; 169, Commentary to art. 11, para. 1.

43 See, e.g., Human Rights Committee (HRComm), General Comment No. 36 on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life, CCPR/C/GC/36, 30 October 2018, §§ 25, 28–30; European Court of Human Rights (ECtHR), Guide on Article 2 of the European Convention on Human Rights: Right to Life, updated on 31 December 2019, para. 101.

44 See, e.g., Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts 1977, 1125 UNTS 3, arts 57–58 (Additional Protocol I); International Committee of the Red Cross (ICRC), Customary IHL Database, Rule 15, available at https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule15.

45 See Section 4 below.

certain international obligations conceived for the 'offline' world equally apply to cyberspace, as a new 'domain' or technology.[46] Secondly, it could be argued that states have, in their practice and expressions of *opinio juris*, actively carved out cyberspace from the scope of application of said duties.

In addressing those possible objections, it is important to note that several states and international institutions have consistently affirmed the application of international law *as a whole* to cyberspace, including, in particular, rules and principles that flow from sovereignty.[47] And this is because rules of general international law apply, by default and across the board, to all areas and types of state activity. This is so to the extent that the activities in question fall within the scope of those rules and exceptions or more specific rules do not displace them.[48] For this reason, several states

[46] See, *mutatis mutandis*, Corn and Taylor, 'Sovereignty in the Age of Cyber', 111 *American Journal of International Law* (2017) 207, at 208 (challenging on a similar basis the applicability of a rule of sovereignty to cyberspace). See also Note from Mr. Gabriel Juárez Lucas, Fourth Vice Minister of the Interior Ministry of the Republic of Guatemala to Luis Toro Utillano, Technical Secretariat, Inter-American Juridical Committee, 4VM.200–2019/GJL/lr/bm, 14 June 2019, cited in Organization of American States (OAS), Improving Transparency – International Law and State Cyber Operations: Fourth Report (Presented by Prof. Duncan B. Hollis), OEA/Ser.Q, CJI/doc. 603/20 rev.1, 5 March 2020, § 21 (hereinafter 'Improving Transparency') (expressing support for the application of international law to cyberspace but noting that there could be areas where 'the novelty of cyberspace does preclude the application of certain international rights or obligations').

[47] See, e.g., Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, 24 June 2013, § 19 (hereinafter 'UN GGE Report 2013'); UN GGE Report 2015, *supra* note 5, §§ 24–28; Hon. Paul C. Ney, Jr, US Department of Defense, General Counsel Remarks at US Cyber Command Legal Conference (2 March 2020), available at www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference; US Government, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (May 2011), at 9, available at https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (hereinafter 'International Strategy for Cyberspace'); Australian Department of Foreign Affairs and Trade (DFAT), 'Australia Non Paper: Case Studies on the Application of International Law in Cyberspace' (2020), at 4, 7–11, available at www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf (hereinafter 'Australia Non Paper'); Jeremy Wright QC MP, UK Attorney General, Speech, 'Cyber and International Law in the 21st Century' (2018), at 3–6, available at www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century; Ministère de la Defense (France), 'Droit international appliqué aux opérations dans le cyberespace', at 6–17, available at www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqué+aux+opérations+Cyberespace.pdf (last visited 10 July 2021); Keynote address by the Minister of Defence of the Kingdom of the Netherlands, Ms. Ank Bijleveld (20 June 2018), available at https://english.defensie.nl/downloads/speeches/2018/06/21/keynote-address-by-the-minister-of-defence-ms.-ank-bijleveld-marking-the-first-anniversary-of-the-tallinn-manual-2.0-on-the-20th-of-june-2018. See similarly Comments by Member States on the Initial Pre-Draft of the OEWG Report, available at www.un.org/disarmament/open-ended-working-group/ (see individual comments from the Czech Republic, at 2; the Netherlands, §§ 17–18; Japan, at 1, 5; Austria, at 2; Germany, at 2–3). See also HRC, Res. 32/13, *supra* note 28.

[48] *S.S. Lotus*, 1927 PCIJ Series A, No. 10, para. 45; ILC, Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law, Report of the Study Group of the International Law Commission Finalized by Martti Koskenniemi, UN Doc A/CN.4/L.682, 13 April 2006, § 120 (hereinafter 'Fragmentation Report'). See also Akande, Coco and de Souza Dias, 'Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond', *EJIL: Talk!* (5 January 2021), available at www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/.

have stressed that rules of international law are technology-neutral, even if questions remain as to *how* they apply to new means of communication.[49] After all, as a means to a variety of ends, ICTs cannot be severed from the activities to which they serve and, consequently, from the rules governing them.

Two key rules deriving from the principle of sovereignty and applying generally in international law are precisely the Corfu Channel and the no-harm principles. Thus, the presumption we ought to proceed from is that they apply to ICTs, in the absence of *leges speciales* to the contrary.[50] In the same vein, the scope of application of IHRL and IHL is broad, only limited by their respective triggers and subject matter.[51] This means that, by default, positive duties established in both regimes apply to cyberspace, in the absence of specific carve-outs excluding ICTs from their scope of application. There is no evidence of such an exception, and admissible derogations from such obligations must be interpreted restrictively, due to their *erga omnes* character.[52]

On the contrary, states have not only invoked general international law, IHRL and IHL but also supported the applicability of different protective obligations in cyberspace, even if in a somewhat fragmented way. For instance, as far back as 2011, the then United States (US) government recognized the application of positive IHRL duties online as well as a duty to prevent cybercrime.[53] Shortly thereafter, the Council of Europe issued a recommendation recognizing the applicability of the no-harm principle to malicious cyber activities.[54] The Explanatory Memorandum adds that this principle

> sets forth a standard of care or due diligence for the protection and promotion of integrity and universality of the Internet . . . . Under such a standard, states are required to take reasonable measures to prevent, manage and respond to significant transboundary disruptions to or interferences with the infrastructure or critical resources of the Internet.[55]

[49] OEWG, Second 'Pre-Draft' Report on Developments in the Field of Information and Telecommunications in the Context of International Security (2020), § 21, available at www.un.org/disarmament/open-ended-working-group/. See also Moynihan, 'The Application of International Law to State Cyberattacks Sovereignty and Non-Intervention', Chatham House Research Paper, December 2019, paras 5–6. See also *Tallinn Manual 2.0*, *supra* note 6, at 31, para. 4; 46, para. 12; *Nuclear Weapons*, Advisory Opinion, 8 July 1996, ICJ Reports (1996), para. 39; ILC, Draft Articles on Prevention, *supra* note 21, at 154, Commentary to Draft Article 3, para. 11; *Responsibilities and Obligations of States with Respect to Activities in the Area*, Advisory Opinion, 1 February 2011, ITLOS Reports (2011) 10, para. 117; Sullivan, *supra* note 3, at 452; Geiss and Lahmann, 'Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention', in K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (2013) 621, at 655.

[50] *Tallinn Manual 2.0*, *supra* note 6, at 31, para. 4; Okwori, 'The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap Between Universal and Differential Approaches for States', *Ethiopian Yearbook of International Law* (2018) 205, at 213; Khanna, 'State Sovereignty and Self-Defence in Cyberspace', 5 *BRICS Law Journal* (2018) 139, at 141. See, generally, *Nuclear Weapons*, Advisory Opinion, 8 July 1996, ICJ Reports (1996), para. 39.

[51] *Nuclear Weapons*, Advisory Opinion, 8 July 1996, ICJ Reports (1996), para. 86.

[52] ILC, Fragmentation Report, *supra* note 48, § 109.

[53] International Strategy for Cyberspace, *supra* note 47, at 10.

[54] Council of Europe, Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet (21 September 2011), available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f8.

[55] 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,

Along with the aforementioned statement by the EU representative in the context of the COVID-19 crisis – which was expressly supported by Turkey, North Macedonia, Montenegro, Serbia, Albania, Bosnia and Herzegovina, Iceland, Liechtenstein, Norway, Ukraine, Moldova and Armenia[56] – several states have recently recognized slightly different iterations of 'cyber due diligence' as a matter of international law. For instance, mirroring the Corfu Channel dictum and rule 6 of the Tallinn Manual, France has recently stated that:

> In accordance with the principle of due diligence, States have the obligation to not knowingly allow their territory to be used to commit *acts prohibited by international law against third States* through the use of cyber means. This obligation also applies to activities conducted in cyberspace by non-state actors situated in the territory or under the jurisdiction of the State in question.[57]

Similarly, Estonia has expressed the view that 'states have to make reasonable efforts to ensure that their territory is not used to *adversely affect the rights of other states*'.[58]

Using different wording, Australia has pointed out that 'to the extent that a state enjoys the right to exercise sovereignty over objects and activities within its territory, it necessarily shoulders corresponding responsibilities to ensure those objects and activities are not used to *harm* other states'.[59] More eloquently, Finland has stated that '[i]t is clear that States have an obligation not to knowingly allow their territory to be used for activities that *cause serious harm to other States*, whether using ICTs or otherwise'.[60]

CM Documents, CM(2011)115-add1, 24 August 2011, § 80 and more extensively §§ 71–84, available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805ccaeb. See also 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 cooperation on cross-border Internet, Strasbourg, December 2010, §§ 59–74, esp. §§ 72–74 (on the standard of due diligence), available at http://humanrightseurope.blogspot.com/2011/01/proposals-for-international-cooperation.html.

56 See Council of the EU, Press Release, *supra* note 2.

57 Comments by Member States on the initial predraft of the OEWG report, *supra* note 47, France, at 3 (emphasis added). Cf. Anne Gueguen, French Deputy Permanent Representative at the UN, Statement at the UNSC Arria-Formula Meeting on Cybersecurity (2020), at 1:35:15 min, available at https://youtu.be/K704P5D1n3E; Ministère de la Defense (France), *supra* note 47, at 10. Cf. Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General, UN Doc. A/74/120, 24 June 2019, at 24 (reply by France); Stratégie internationale de la France pour le numérique (2017), at 32, available at www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf.

58 President of the Republic [of Estonia] at the opening of CyCon 2019 (29 May 2019), available at www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html (emphasis added).

59 Australia Non Paper, *supra* note 47, at 8 (emphasis added). See also Australia, DFAT, Australia's International Cyber Engagement Strategy, at 90, Annex A: Australia's position on how international law applies to state conduct in cyberspace (2019), available at https://www.internationalcybertech.gov.au/about/2017-International-Cyber-Engagement-Strategy.

60 Janne Taalas, Ambassador, Statement at the second session of the open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security (February 2020), available at https://ccdcoe.org/uploads/2018/10/Statement-on-International-Law-by-Finnish-Ambassador-Janne-Taalas-at-2nd-session-of-OEWG.pdf (emphasis added).

It has also recognized that 'each State has to protect individuals within its territory and subject to its jurisdiction from interference with their rights by third parties'.[61] And, in what seems to combine different rules, The Netherlands have posited that:

> The principle is articulated by the International Court of Justice, for example, in its judgment in the Corfu Channel Case, in which it held that states have an obligation to act if they are aware or become aware that their territory is being used *for acts contrary to the rights of another state*. … It is generally accepted that the due diligence principle applies only if the state whose right or rights have been violated suffers *sufficiently serious adverse consequences*.[62]

Similar statements have been made by the Czech Republic,[63] the Republic of Korea,[64] Japan,[65] Austria,[66] the Dominican Republic,[67] Chile, Ecuador, Guatemala, Guyana and Peru.[68] Taken together, they overshadow the contrary statements made so far by Argentina, Israel, New Zealand and the United Kingdom, which either reject or question the applicability of due diligence duties to ICTs.[69] Most importantly, they strongly support the view that *existing* protective obligations containing a due diligence standard are fully applicable to ICTs, even if their specific implementation requires additional guidance.

That said, two important questions remain open: (i) whether an all-encompassing 'principle of due diligence' exists *generally* in international law; and (ii) whether a single protective obligation – with a corresponding due diligence standard – exists *specifically* for cyberspace.[70] In particular, some have suggested that rule 6 of the Tallinn Manual and similar cyber-articulations of the concept of due diligence are *lex ferenda*[71] or mere interpretations of how an existing, wide-ranging 'due diligence

[61] *Ibid.*

[62] Government of the Netherlands, Letter from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace (5 July 2019), Appendix: International law in cyberspace at 4–5, available at www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace (hereinafter 'Netherlands, Letter of 5 July 2019') (emphases added).

[63] Czech Republic, *supra* note 47, at 3.

[64] Comments by Member States on the initial pre-draft of the OEWG report: Republic of Korea, *supra* note 47, at 2.

[65] Ministry of Foreign Affairs of Japan, Basic Position of the Government of Japan on International Law Applicable to Cyber Operations (28 May 2021), available at https://www.mofa.go.jp/policy/page3e_001114.html, at 5.

[66] Comments by Member States on the initial pre-draft of the OEWG report: Austria, *supra* note 47, at 2–5.

[67] H.E. Mr. José Singer Weisinger, Dominican Republic's Ambassador and Special Envoy to the Security Council, Statement (22 May 2020), available at https://vm.ee/sites/default/files/Estonia_for_UN/22-5-2020_cyber_stability_and_conflict_prevention_-3.pdf.

[68] OAS, Improving Transparency, *supra* note 46, § 58. See also *ibid.*, §§ 56ff.

[69] *Supra* note 8.

[70] See, e.g., The Netherlands, Letter of 5 July 2019, *supra* note 62, Appendix, at 4 (acknowledging that 'it should be noted that not all countries agree that the due diligence principle constitutes an obligation in its own right under international law. The Netherlands, however, does regard the principle as an obligation in its own right, the violation of which may constitute an internationally wrongful act').

[71] See Schmitt, '"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law', 19 *Chicago Journal of International Law* (2018) 30, at 51. See also *Tallinn Manual 2.0*, *supra* note 6, at 32, para. 6; International Strategy for Cyberspace, *supra* note 47, at 10 (listing 'Cybersecurity Due Diligence' as an emerging norm specific to cyberspace); Argentina's OEWG Statement, *supra* note 8.

obligation' should apply to cyberspace.[72] They have pointed to several reasons of policy behind states' reluctance to commit to a new rule. For instance, states may fear that a fine-grained due diligence standard for cyberspace would be too burdensome to implement and could stifle its necessary flexibility.[73] Alternatively, such a new obligation may put in question the applicability and binding character of existing ones.[74] It is also possible that, by widening the scope of unlawful acts in cyberspace, a new protective 'cyber due diligence' obligation could increase resort to countermeasures and litigiousness among states.[75]

Perhaps the choice of using 'due diligence' to label a range of duties is misleading: its simplicity masks the complexity and diversity of protective obligations requiring diligent behaviour to prevent, halt and redress certain harms. Part of the confusion also seems to arise from the framing of ICTs as a new space or 'domain', rather than a new set of information and communication tools.[76] Nevertheless, the important takeaway is this: the uncertainty surrounding a general principle or a cyber-specific version of due diligence does not mean that cyberspace is a 'duty-free zone'. For, however we label it, an existing patchwork of primary 'protective obligations' already requires states to behave diligently in preventing, halting and redressing different types of harmful cyber operations.

4 Four Sets of Protective Obligations in Cyberspace

A *The Corfu Channel Principle: A Duty to Prevent Cyber Acts Contrary to the Rights of Other States*

The first protective obligation whose applicability in cyberspace has found support among states[77] and commentators[78] is the 'well-recognized' Corfu Channel principle,

[72] See, e.g., Milanovic and Schmitt, 'Cyber Attacks and Cyber (Mis)information Operations during a Pandemic', 11 *Journal of National Security Law & Policy* (2020) 247, at 280 (arguing that '[t]his obligation is simply the cyber application of a *wide-ranging* due diligence positive obligation under general international law requiring a state to stop harm to the rights of other states emanating from its territory', (emphasis added)); Comments by Member States on the initial pre-draft of the OEWG report, *supra* note 47, France (at 1–2); Czech Republic (at 3).

[73] Jensen and Watts, *supra* note 8, at 1574; Adamson, *supra* note 8, at 55, § 12.

[74] Comments by Member States on the initial pre-draft of the OEWG report, *supra* note 47, Austria (at 2); Australia (at 2–3, item C2).

[75] Jensen and Watts, *supra* note 8, at 1573–1574.

[76] See Akande, Coco, and de Souza Dias, *supra* note 48.

[77] See *supra* notes 54–68.

[78] See, e.g., *Tallinn Manual 2.0*, *supra* note 6, at 35–36, para. 21; Milanovic and Schmitt, *supra* note 72, at 280; Schmitt, 'In Defense of Due Diligence in Cyberspace', 125 *Yale Law Journal Forum* (2015) 68; Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?', 14 *Baltic Yearbook of International Law* (2014) 23, at 25–26; Kulesza, 'Due Diligence in International Internet Law', *Journal of Internet Law* (2014) 24, at 27–28; Geiss and Lahmann, *supra* note 49, at 635; Gross, 'Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents', 48 *Cornell International Law Journal* (2015) 481, at 494; Ney and Zimmermann,

requiring states 'not to allow knowingly its territory to be used for *acts contrary to the rights of other States*'.[79] This duty is a natural corollary of states' sovereign rights over their territory and, in essence, requires them to protect the rights of other states therein.[80] The obligation covers not only acts that directly violate the rights of third states, including their rights to territory and property, but also those of their nationals, even when abroad.[81] It comprises a duty to both *prevent* and *stop* the harmful acts in question[82] and arises as soon as a state knows or should have known[83] that such act *originates* from or *transits* through its territory.[84] Though in essence a preventive duty, the obligation is only breached when the harm materializes.[85] In a sense, this makes it an obligation without sanction for non-compliance, unless actual harm occurs. Often seen as a shortcoming, this norm structure may be explained by the need to encourage states to continuously prevent harm before their responsibility can be engaged.

Rule 6 of the Tallinn Manual seems to contemplate a cyber-specific articulation of the Corfu Channel principle.[86] This formulation – which has been picked up by some states[87] – has four noteworthy features: the type of harm envisaged (Section 4.A.1); the threshold of harm (Section 4.A.2); the scope of preventive duties (Section 4.A.3); and the knowledge requirement (Section 4.A.4).

1 Type of Harm

The Commentary to Rule 6 of the Tallinn Manual posits that an act which 'affects the rights of other states' should be understood as an internationally wrongful act.[88]

'Cyber-Security Beyond the Military Perspective: International Law, "Cyberspace", and the Concept of Due Diligence', 58 *GYIL* (2015) 51, at 61–62; Walter, 'Obligations of States Before, During, and After a Cyber Security Incident', 58 *GYIL* (2015), 67, at 73–76; Dörr, 'Obligations of the State of Origin of a Cyber Security Incident', 58 *GYIL* (2015), 87, at 91–92; Jensen and Watts, *supra* note 8, at 1565–1566.

79 *Corfu Channel*, Judgment, 9 April 1949, ICJ Reports (1949), at 22 (emphasis added).

80 *Island of Palmas*, Award, 4 April 1928, II RIAA 829 (1928), ICGJ 392 (PCA 1928), at 839. See also Australia Non Paper, *supra* note 47, at 8.

81 *Island of Palmas*, Award, 4 April 1928, II RIAA 829 (1928), ICGJ 392 (PCA 1928), at 839; *Affaire des biens britanniques au Maroc espagnol (Spain v United Kingdom)*, 2 RIAA (1925) 615, at 643–644.

82 See, *mutatis mutandis*, *Case Concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgment, 24 May 1980, ICJ Reports (1980) 3, paras 63, 68.

83 *Corfu Channel*, Judgment, 9 April 1949, ICJ Reports (1949), at 18. On the requirement of knowledge as applied to cyberspace, see *Tallinn Manual 2.0*, *supra* note 6, at 40–41.

84 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States)*, Judgment, 27 June 1986, ICJ Reports (1987) 14, para. 157.

85 See ARSIWA, *supra* note 20, art. 14(3). See also *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-Herzegovina v. Yugoslavia)*, Judgment, 26 February 2007, ICJ Reports 2007, at 43, para. 431 (hereinafter '*Bosnian Genocide*'); Bannelier-Christakis, *supra* note 78, at 37. See *contra* Antonopoulos, 'State Responsibility in Cyberspace', in N. Tsagourias and R. Buchan (eds), *Research Handbook on International Law and Cyberspace* (2015) 55, at 69.

86 *Tallinn Manual 2.0*, *supra* note 6, at 30.

87 See, e.g., Comments by Member States on the initial pre-draft of the OEWG report: France, *supra* note 47, at 3; The Netherlands, Letter of 5 July 2019, *supra* note 62, Appendix, at 4.

88 *Tallinn Manual 2.0*, *supra* note 6, at 34, Commentary to Rule 6, para. 17. See also Johanna Weaver, Submission of Australia's independent expert to the United Nations Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security (2020), at 4, available at

It also notes that this ought to include not only breaches of international law attributable to States, but also conduct that *would have been* unlawful *if* committed by the 'host' state, no matter its source.[89] But while the Corfu Channel dictum recognizes state responsibility for lack of diligence in preventing or stopping acts of non-state actors regardless of attribution,[90] no reference is made to either acts merely *affecting* the rights of other states or fully fledged *internationally wrongful acts*, i.e. breaches of international law"attributable to a state. Instead, the language used in Corfu Channel is that of '*acts contrary to the rights of other states*'.[91] In our view, this language does not fully mirror the two concepts featuring in Rule 6 of the Tallinn Manual 2.0 but perhaps sits in between them.

Although most acts contrary to the rights of other states are internationally wrongful acts, the overlap is not complete. First, not all acts committed by non-state groups which are contrary to the rights of other states also constitute internationally wrongful acts or would have done so if committed by the territorial state.[92] The Tallinn Manual 2.0 also does not clarify whether, in speculating if the conduct *would have been* unlawful if committed by the host state, one must consid"r the concrete circumstances prevailing at the time or the obligations of the host state *in abstracto*.[93] A second difference may concern acts that are not unlawful given the existence of circumstances precluding wrongfulness but that would still entitle the 'victim' state to claim compensation for a material loss.[94]

Thus, the framing of the type of harm covered by the Corfu Channel principle as 'internationally wrongful acts' is not entirely accurate. And neither is its qualification as 'acts that affect the rights of other states'. This is because not all acts merely affecting the rights of third states – such as certain instances of cyber espionage[95] – necessarily contravene their rights. Furthermore, acts covered by the Corfu Channel principle need not result in physical damage.[96] This is particularly important in cyberspace, where many harms have no direct material impact yet may hamper the operation of governmental or private functions, such as disruptions of financial or media services.[97]

---

www.dfat.gov.au/sites/default/files/submission-by-australias-representative-to-the-gge-norm-implementation-may-2020.pdf; The Netherlands, Letter of 5 July 2019, *supra* note 62, Appendix, at 4; Okwori, *supra* note 50, at 219–220; Sander, 'Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections', 18 *Chinese Journal of International Law* (2019) 1, at 25–26; Milanovic and Schmitt, *supra* note 72, at 280.

89 *Tallinn Manual 2.0*, *supra* note 6, at 35–36, para. 21.

90 See *Affaire des biens britanniques au Maroc espagnol (Spain v. United Kingdom)*, 2 RIAA (1925) 615, at 643–644; Koivurova, *supra* note 9, para. 2; Dörr, *supra* note 78, at 90; Kolb, *supra* note 37, at 119.

91 *Corfu Channel*, Judgment, 9 April 1949, ICJ Reports (1949), at 22.

92 For instance, during a cross-border non-international armed conflict, the targeting of foreign enemy combatants by a non-state group is contrary to the rights of the foreign state to protect their nationals, yet this may not amount to an internationally wrongful act if committed by the host state itself.

93 *Tallinn Manual 2.0*, *supra* note 6, at 35–36, paras 18–22.

94 ARSIWA, *supra* note 20, art. 27.

95 See Section 4.A.2.

96 Kolb, *supra* note 37, at 121; The Netherlands, Letter of 5 July 2019, *supra* note 62, at 5.

97 See *Tallinn Manual 2.0*, *supra* note 6, at 38.

An example of cyber activities 'contrary to the rights of other States' may be found in the United Kingdom's recent condemnation of 'irresponsible activity being carried out by criminal groups' and 'cyberattacks by States and non-States actors' during the COVID-19 pandemic.[98] The acts in question consisted of 'malicious cyber campaigns targeting international healthcare and medical research organizations involved in the coronavirus response', which were clearly contrary to the rights of targeted states, regardless of any material harm caused.

2 Threshold of Harm?

Rule 6 of the Tallinn Manual is said to be engaged only if an internationally wrongful act has 'serious adverse consequences' for other states.[99] This threshold of harm is not found in pre-existing iterations of the Corfu Channel principle. Instead, it seems to have been borrowed from the no-harm principle,[100] which requires *significant* transboundary harm but not necessarily an act contrary to the rights of other states. Like much of the existing literature on due diligence,[101] the Manual seems to have merged the two principles into one single rule or principle requiring due diligence in cyberspace.[102]

However, that is not to say that a failure to prevent or halt any cyber harm, regardless of its gravity, amounts to a breach of the Corfu Channel principle. States are not responsible for failing to avoid minor or negligible disruptions, such as the temporary defacement of non-essential government websites. But this is not because the principle contains a specific harm threshold. Rather, it is because those harms may not be contrary to the rights of other states.[103] For instance, in many circumstances, mere exfiltration or corruption of data – according to some – may not be contrary to the victim state's sovereign rights over its territory[104] or its right not to be subjected to foreign

[98] Press Release, 'UK Condemns Cyber Actors Seeking to Benefit from Global Coronavirus Pandemic' (5 May 2020), available at www.gov.uk/government/news/uk-condemns-cyber-actors-seeking-to-benefit-from-global-coronavirus-pandemic.

[99] *Ibid.*, at 36–37, paras 25–27; 39, para. 33. See also Okwori, *supra* note 50, at 218–219; Milanovic and Schmitt, *supra* note 72, at 279. See also The Netherlands, Letter of 5 July 2019, *supra* note 62, Appendix, at 5; Comments by Member States on the initial pre-draft of the OEWG report: Canada, *supra* note 47, at 3.

[100] Schmitt, *supra* note 71, at 54.

[101] See, e.g., Couzigou, 'Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations', 32 *International Review of Law, Computers & Technology* (2018) 37; Okwori, *supra* note 50, at 208–213; Geiss and Lahmann, *supra* note 49, at 635; Gross, *supra* note 78, at 494; Ney and Zimmermann, *supra* note 78, at 61–62; Walter, *supra* note 78, at 73–76; Dörr, *supra* note 78, at 91–92; Brunée and Meshel, *supra* note 21, at 133–135; Jensen and Watts, *supra* note 8, at 1565–1566.

[102] *Tallinn Manual 2.0*, *supra* note 6, at 30–32, paras 1–5. See also Milanovic and Schmitt, *supra* note 7274, at 280.

[103] Walton, 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law', 126 *Yale Law Journal* (2016) 1460, at 1502; Crootof, 'International Cybertorts: Expanding State Accountability in Cyberspace', 103 *Cornell Law Review* (2018) 565, at 565–567, 597–599, 606–607.

[104] See Corn and Taylor, *supra* note 46, at 209–210. But see *Tallinn Manual 2.0*, *supra* note 6, at 18–19 and 171, para. 10 (noting that although most acts of cyber espionage are lawful, they may constitute a breach of sovereignty if physically conducted on the territory of the victim state and attributable to another state). See also R. Buchan, *Cyber Espionage and International Law* (2019), at 51.

intervention.[105] Conversely, lack of due diligence in preventing or stopping malicious cyber operations that interfere with a state's inherently sovereign functions or *domaine reservé*, such as its ability to establish public health policies or to hold elections, might breach the Corfu Channel principle. And this includes acts occurring entirely within the duty-bearer's territory, as the Corfu Channel principle does not require the physical crossing of a territorial boundary.[106]

3 Scope of Preventive Duties

Drawing on the duty to prevent genocide, the group of experts involved in Tallinn 2.0 rejected the view that states have a 'general duty of prevention', that is, a duty to prevent *future* malicious cyber operations.[107] For the Tallinn 2.0 experts, the Corfu Channel principle only applies to *ongoing*, or at most *imminent*, operations, at least as far as cyberspace is concerned.[108] This would limit the scope of the duty to an obligation to simply halt harmful cyber operations.[109] As a consequence, when discharging this duty, states would not be required to adopt strictly preventive, *ex ante* measures, such as continuous supervision or monitoring of their networks.[110]

This view has been justified by the current lack of technical feasibility to prevent online harms, given their frequency and speed, as well as privacy concerns.[111] But this misses the point. Protective obligations, including the Corfu Channel principle, are inherently flexible. They depend on the capacity and position of each state to prevent or halt the harm in question, whether the cyber operation originates from or transits through its territory.[112] Thus, a state is not required to do the impossible, and different states may be required to adopt different measures in different circumstances. State practice in this respect reveals that a range of measures has been adopted to prevent

[105] *Tallinn Manual 2.0*, *supra* note 6, at 36, para. 23.

[106] This position seems to have been implicitly endorsed in *Tallinn Manual 2.0*, *supra* note 6, at 39, para. 32.

[107] *Ibid.*, at 31, para. 5; 41–42, para. 42; 44–45, paras 7, 10.

[108] *Ibid.*, at 43–44, paras 3–4. See also Okwori, *supra* note 50, at 216.

[109] *Tallinn Manual 2.0*, *supra* note 6, at 44–45, para. 7.

[110] *Ibid.*, at 44–45, paras 7, 10; Couzigou, *supra* note 101, at 50–51; Okwori, *supra* note 50, at 215; Jensen and Watts, *supra* note 8, at 1566; Takano, 'Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications', 36 *Laws* (2018) 7, at 8. See also ILA Study, *supra* note 14, at 7–8; Estonia, *supra* note 58; Comments by Member States on the initial pre-draft of the OEWG report: Canada, *supra* note 47, at 3; Comments by Member States on the initial pre-draft of the OEWG report: Ecuador, *supra* note 47, at 2.

[111] *Tallinn Manual 2.0*, *supra* note 6, at 45, para. 8. See also Okwori, *supra* note 50, at 215; Crootof, *supra* note 103, at 611, Goldsmith, *Cybersecurity Treaties: A Skeptical View – Future Challenges Essay* (2011), at 9–10, available at https://www.hoover.org/sites/default/files/research/docs/futurechallenges_goldsmith.pdf.

[112] *Tallinn Manual 2.0*, *supra* note 6, at 47, paras 16–18; Buchan, *supra* note 1, at 441–442; Bannelier-Christakis, *supra* note 78, at 37; Dörr, *supra* note 78, at 95. See also Ecuador, *supra* note 47, at 2; The Netherlands, Letter of 5 July 2019, *supra* note 62, Appendix, at 5; Australia Non Paper, *supra* note 47, at 8; Comments by Member States on the initial pre-draft of the OEWG report: Canada, *supra* note 47, at 3. On the obligations of transit states, see *Tallinn Manual 2.0*, *supra* note 6, at 33–34, para. 34.

harmful cyber operations. These have included cyber-threat monitoring[113] and the issuance of alerts and advisories to address software or hardware vulnerabilities.[114]

Yet such flexibility is no excuse for inaction. A logical prerequisite to protective obligations *of conduct* is a separate obligation to put in place the minimum governmental infrastructure that is reasonable in the circumstances, enabling a state to exercise the necessary degree of diligence.[115] This is likely an obligation *of result*, i.e. a baseline governmental infrastructure *must* be established.[116] Indeed, if a state could simply claim that it has exercised its best efforts for this purpose, the main duty to prevent harm could be easily evaded. However, the content of such capacity-building obligation – the result required from each state – does not seem to be fixed, but dependent on the circumstances, in particular, available human and financial resources.

Thus, the Corfu Channel principle contains two distinct but interconnected limbs.[117] First, there is an obligation to set up a minimal state apparatus – a core 'capacity-building' duty. Recent state practice in the cyber context indicates that such duty would include the adoption and implementation of an adequate national legal framework tackling cybercrime and misuse of ICTs.[118] Secondly, there is an obligation *of conduct* to exercise due diligence to prevent and halt potential or actual cyber operations contrary to the rights of other states, to the extent of a state's capacity to act in the circumstances. Thus, a state's capacity to act not only triggers its obligation of conduct but also limits and modulates the measures it is required to adopt. However, as with other protective duties, required measures may change on the basis of new technological developments.[119] For instance, if a state has or acquires cyber monitoring technologies enabling it to anticipate and prevent certain malicious cyber operations, these must be used as far as possible.[120] While these technologies may raise concerns about privacy and other rights, it suffices to note that the implementation of

[113] See, e.g., Cybersecurity Law (promulgated by the Standing Committee of the National People's Congress, 7 November 2016, effective 1 June 2017), arts. 21(3), 51 (China); UK Network and Information Systems Regulations 2018, 10 May 2018, Part II, s. 5(2)(a); Japan Cybersecurity Strategy (27 July 2018), at 27–29, 31, 35.

[114] See, e.g., US Cybersecurity & Infrastructure Security Agency, Alert: Technical Approaches to Uncovering and Remediating Malicious Activity, AA20-245A (1 September 2020), available at https://us-cert.cisa.gov/ncas/alerts/aa20-245a; Canada's Implementation of the 2015 GGE Norms, at 5, available at www.un.org/disarmament/wp-content/uploads/2019/11/canada-implementation-2015-gge-norms-nov-16-en.pdf (last visited 17 July 2021).

[115] See Buchan, *supra* note 1, at 436–437; Kolb, *supra* note 37, at 127, Couzigou, *supra* note 101, at 50–51; Takano, *supra* note 110, at 9. On the no-harm principle, see ILC, Draft Articles on Prevention, *supra* note 21, at 155, Commentary to art. 3, paras 15–17.

[116] Pisillo-Mazzeschi, *supra* note 14, at 26; Buchan, *supra* note 1, at 434–439.

[117] Pisillo-Mazzeschi, *supra* note 14, at 26–27.

[118] See, e.g. International Cyber Engagement Strategy, Annex B: Australian Implementation of Norms of Responsible State Behaviour in Cyberspace (2019), sub (c), available at https://www.internationalcybertech.gov.au/sites/default/files/2020-12/how-australia-implements-the-ungge-norms.pdf; Canada's Implementation of the 2015 GGE Norms, *supra* note 114, at 4–5.

[119] See *supra* note 49.

[120] See *supra* note 110.

due diligence measures under the Corfu Channel principle must be in line with international human rights law and other rules of international law.[121]

4 Knowledge Requirement

In any event, the obligation to act in accordance with the Corfu Channel principle is only activated when a state knows, or should have known, about a *serious* risk that an unlawful cyber operation will take place, no matter how remote such a risk is.[122] Thus, the decisive factor is how much information and certainty a state possesses about the harmful act in question, rather than how imminent or proximate it is.[123] The same applies to transit states, to the extent that they have actual or constructive knowledge of the risk of an unlawful cyber operation, as well as the capacity to prevent it.[124]

At the same time, it does not appear that the Corfu Channel principle imposes on states a duty to actively seek knowledge of acts emanating from or transiting through their territory which would be contrary to the rights of other states.[125] What it does require is the minimum governmental infrastructure or capacity *enabling* states to acquire such knowledge.[126] Yet it has been suggested that the knowledge requirement may be proven by a (rebuttable) presumption when an unlawful cyber operation originates in non-commercial cyber infrastructure under a state's exclusive governmental control.[127] This could prevent states from easily evading their protective obligations by denying knowledge of a certain unlawful cyber operation.

In short, 'the more states *can* do, the more they must do',[128] and great responsibility follows inseparably from great power,[129] to the extent that such power permits. Therefore, complying with the Corfu Channel principle in cyberspace should not be an insurmountable feat: it simply requires states to build the minimum capacity that is reasonably expected of them, as well as to employ this capacity diligently in *trying* to protect the rights of other states, as far as possible.[130] In many circumstances, reporting and sharing information about cyber incidents will suffice.[131]

[121] See Bannelier-Christakis, *supra* note 78, at 31; Dörr, *supra* note 78, at 95.

[122] See Kolb, *supra* note 37, at 123–124; *Tallinn Manual 2.0*, *supra* note 6, at 45, para. 9 and *ibid.*, at 44–45, para. 7, citing *Bosnian Genocide*, Judgment, 26 February 2007, ICJ Reports 2007, *supra* note 85, para. 431.

[123] See, *mutatis mutandis*, *Bosnian Genocide*, Judgment, 26 February 2007, ICJ Reports 2007, para. 436.

[124] Similarly, see Couzigou, *supra* note 101, at 43, 47; Buchan, *supra* note 1, at 441. See *contra* Reinisch and Beham, *supra* note 11, at 106–107; Okwori, *supra* note 50, at 226–227.

[125] But international human rights law might impose a duty to actively seek knowledge of certain threats to human rights. See Section 3.C.

[126] See *supra* note 115.

[127] Heintschel von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace', in C. Czosseck, R. Ottis and K. Ziolkowski (eds), *2012 4th International Conference on Cyber Conflict* (2012) 7, at 17.

[128] Heieck, *Symposium: A Duty to Prevent Genocide – Due Diligence Obligations among the P5 (Part One)* (2018), available at http://opiniojuris.org/2018/12/10/symposium-a-duty-to-prevent-genocide-due-diligence-obligations-among-the-p5-part-one/ (emphasis added).

[129] *Collection générale des décrets rendus par la Convention Nationale*: *Mois de mai 1793* (1793), at 72. The adage has been popularized by the Spiderman comic books.

[130] See, similarly, Kolb, *supra* note 37, at 123.

[131] Gross, *supra* note 78, at 506. See also Secretariat Général de la Défense et la Sécurité Nationale (France), Revue stratégique de cyberdéfense (12 March 2018), at 83–84, available at www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/.

B *The Duty to Prevent and Redress Significant Transboundary Cyber Harm*

Despite their similarities, particularly a common 'capacity-to-act' requirement, the no-harm and Corfu Channel principles should be distinguished, given their distinct elements and legal consequences.[132] There are at least four significant differences between the two primary obligations: i) the type of harm; ii) the threshold of harm; iii) the knowledge requirement; and iv) the legal consequences of a failure to comply with the duty.

1 Type of Harm

Unlike the Corfu Channel principle, the no-harm principle does not require the infliction of an act contrary to the rights of other states but covers any 'significant transboundary harm' or the risk thereof, even if caused by lawful activities or no state right is undermined.[133] In 'cyberspace' as in more traditional 'spaces', such as land, air and sea, the crossing of a border occurs when harm is caused or felt in the territory of – or in other places or infrastructures under the jurisdiction or control of – a state other than the state of origin.[134] This is so to the extent that ICTs remain grounded in physical spaces or structures and are used or controlled by human beings, even if certain online activities cause primarily non-physical effects.[135]

While some have questioned whether this obligation applies outside of the environmental legal framework, there are strong reasons to suggest that it covers *any* type of transboundary harm,[136] including harm caused through ICTs. In particular, the *Trail Smelter* arbitral tribunal found that the obligation not to cause transboundary harm includes any 'injurious act' to the territory of another state, persons or property therein.[137] In doing so, it looked at precedents dealing not only with environmental

[132] See ILC, Summary Record of the 1251st Meeting, Topic: State Responsibility, A/CN.4/SR.1251, Extract from the Yearbook of the International Law Commission 1974 vol. 1, available at https://legal.un.org/ilc/documentation/english/summary_records/a_cn4_sr1251.pdf (last accessed 17 July 2021), at 7 (noting that '[i]n any case it was essential to make a very *clear distinction* between *responsibility for wrongful activities* and *liability for lawful activities liable to cause damage*. In the case of wrongful activities, *damage* was often an important element, but it was *not absolutely necessary* as a basis for international responsibility. On the other hand, *damage was an indispensable element for establishing liability* for lawful, but injurious activities' (emphasis added). See also Crootof, *supra* note 103, at 600; Walton, *supra* note 103, at 1486–1487; Sander, *supra* note 88, at 49.

[133] ILC, Draft Articles on Prevention, *supra* note 21, at 150, Commentary to Article 1, para. 6; 152, Commentary to art. 2, para. 5. See also Koivurova, *supra* note 9, para. 11; Crootof, *supra* note 103, at 600.

[134] ILC, Draft Articles on Prevention, *supra* note 21, at 151–153, art. 2(c) and Commentary, paras 8–9.

[135] Akande, Coco and de Souza Dias, *supra* note 48. See also Schmitt, 'Israel's Cautious Perspective on International Law in Cyberspace: Part I (Methodology and General International Law', *EJIL: Talk!* (17 December 2020), available at www.ejiltalk.org/israels-cautious-perspective-on-international-law-in-cyberspace-part-i-methodology-and-general-international-law/.

[136] See ILC, Draft Articles on Prevention, *supra* note 21, at 148–149; Crootof, *supra* note 103, at 603–604; Walton, *supra* note 103, at 1465, 1479–1481; Sander, *supra* note 88, at 51.

[137] *Trail Smelter*, (*United States v. Canada*) (1941) 3 RIAA 1911, at 1963.

hazards but also the use of weapons and the treatment of aliens.[138] Similarly, according to the ICJ, the no-harm principle is a manifestation of the general principle of prevention and therefore closely relates to the Corfu Channel rule.[139] Granted, this general finding was made in the context of a state's obligation 'to use all the means at its disposal in order to avoid activities which take place in its territory, or in any area under its jurisdiction, causing significant damage to the environment of another State'.[140] Yet, that the Court specifically highlighted the existence of this duty, 'now part of the corpus of international law relating to the environment',[141] as was relevant to that case, by no means exhausts or negates the *general* applicability of the no-harm principle beyond the environmental realm. In fact, the ILC has clarified that its Draft Articles on Prevention of Transboundary Harm apply to 'harm caused to persons, property *or* the environment', which includes 'detrimental effects on matters such as, for example, human health, industry, property, environment or agriculture'.[142]

For those reasons, many commentators have persuasively expressed the view that the no-harm principle applies to a range of harms committed through ICTs, whether or not they are contrary to the rights of other states.[143] Admittedly, many harmful cyber operations *will* be contrary to at least one rule of international law and will likely be contrary to the rights of other states. In particular, if sovereignty is a standalone rule of international law, intrusions into governmental networks or systems by another state that cause physical or functional harm in another state's territory may breach such rule.[144] Likewise, coercive cyber interference with a state's exclusive governmental functions, such as its ballot-counting or national banking systems, would violate the principle of non-intervention.[145] And to the extent that those cyber incursions violate the rights of individuals, such as their right to free elections, privacy or property, they would likely violate international human rights law.[146] This should be

[138] *Ibid.*, at 1963–1965.

[139] *Pulp Mills*, Judgment, 20 April 2010, ICJ Reports (2010), para. 101.

[140] *Ibid.*

[141] *Ibid.*, citing *Nuclear Weapons*, Advisory Opinion, 8 July 1996, ICJ Reports (1996), para. 29.

[142] ILC, Draft Articles on Prevention, *supra* note 21, art. 2, at 153, para. 8; Commentary, at 152, para. 4 (emphasis added). See also Robert Q. Quentin-Baxter, Special Rapporteur, Fourth Report on International Liability for Injurious Consequences Arising out of Acts Not Prohibited by International Law, UN Doc. A/CN.4/373 and Corr.1&.2 (27 June 1983), para. 17 (clarifying that 'there was never an intention to propose a reduction in the scope of the topic to questions of an ecological nature').

[143] See, e.g., Crootof, *supra* note 103, at 603–604; Walton, *supra* note 103, at 1480–1482, 1497; Sander, *supra* note 88, a 49–50; Reinisch and Beham, *supra* note 11, at 104–106; Dörr, *supra* note 78, at 93; Buchan, *supra* note 1, at 439–452; Okwori, *supra* note 50, at 210; Takano, *supra* note 110. See also Interim Report of the Ad-Hoc Advisory Group on Cross-Border Internet, *supra* note 55, paras 60–65.

[144] *Tallinn Manual 2.0*, *supra* note 6, at 19–22; Schmitt and Vihul, 'Respect for Sovereignty in Cyberspace', 95 *Texas Law Review* (2017) 1639, at 1648–1649. Granted, controversies as to the existence and extent of such rule may lead to diverging views about the occurrence of 'harm'. This does not deny, however, that if such harm may be established the 'no-harm' principle would apply.

[145] See, e.g., Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention', in J. D. Ohlin et al. (eds), *Cyber War: Law and Ethics for Virtual Conflicts* (2015) 250, at 257. But see Sander, *supra* note 88, at 20.

[146] Sander, *supra* note 88, at 35–43.

true at least for *negative* human rights obligations,[147] for which a state's jurisdiction may be triggered by the exercise of control over the activity in question,[148] the digital communications infrastructure[149] or the enjoyment of the victim's human rights,[150] regardless of physical proximity between the perpetrator and the victim.

However, no rule of international law needs to be breached or contravened for the no-harm principle to apply.[151] This gives the principle a potentially wide scope of application which is particularly well-suited for cyberspace, where debates continue as to the nature of sovereignty, jurisdiction and prohibited intervention.[152] It may be the only applicable international rule requiring states to prevent, stop and redress certain low-intensity cyber operations.[153] Although the no-harm principle requires the crossing of an international boundary,[154] it is not limited to physical harms.[155] Often referred to as 'international cybertorts',[156] these transboundary operations may include substantial financial loss, functional and/or physical damage to private networks or systems, data corruption or loss, reputational injuries and political consequences.[157]

2 *Threshold of Harm*

At the same time, the no-harm principle is only engaged by *significant* transboundary harm or the risk thereof. In the words of the ILC: 'It is to be understood that *"significant" is something more than "detectable" but need not be at the level of "serious" or "substantial"*. The harm must lead to a *real* detrimental effect on matters such as, for example, human health, industry, property, environment or agriculture in other States'.[158] 'Significant harm', in this context, encompasses 'the combined effect of the

[147] See M. Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (2011), at 209; Sander, *supra* note 88, at 39–43. On extraterritorial jurisdiction over online harms, see Section 4.C.1.

[148] *Sergio Euben Lopez Burgos v. Uruguay*, HRComm Communication No. 52/1979, UN Doc. CCPR/C/13/D/52/1979, 29 July 1981, § 12.3; *Lilian Celiberti de Casariego v. Uruguay*, HRComm Communication No 56/1979, UN Doc. CCPR/C/13/D/56/1979, 29 July 1981, § 10.3.

[149] Report of the Office of the UN High Commissioner for Human Rights: The Right to Privacy in the Digital Age, UN Doc. A/HRC/27/37, 30 June 2014, § 34.

[150] HRComm, General Comment No. 36, *supra* note 43, § 63; ECtHR, *Issa and Others v. Turkey*, Appl. no. 31821/96, Judgment of 16 November 2004, para. 71; ECtHR, *Jaloud v. The Netherlands*, Appl. no. 47708/08, Judgment of 20 November 2014, para. 152.

[151] Walton, *supra* note 103, at 1486. See also Finland, *Statement by Ambassador Janne Taalas*, *supra* note 61, at 2.

[152] Crootof, *supra* note 103, at 592–593; Sander, *supra* note 88, at 18–24, 52.

[153] Walton, *supra* note 103, at 1497–1499, 1512.

[154] ILC, Draft Articles on Prevention, *supra* note 21, at 152–153, art. 3(c)–(e) and Commentary, paras 9–12.

[155] According to the ILC, the Draft Articles on Prevention were limited to physical harms 'to bring this topic within a manageable scope'. See *ibid.*, at 151; Commentary to art. 1, para. 16; *Trail Smelter* (*United States v. Canada*) (1941) 3 RIAA 1911, at 1926–1927; *Nuclear Weapons*, Advisory Opinion, 8 July 1996, ICJ Reports (1996), paras 29 and 36. See also Crootof, *supra* note 103, at 603; Walton, *supra* note 103, at 1482; Buchan, *supra* note 1, at 449–450; Takano, *supra* note 110, at 1.

[156] See Crootof, *supra* note 103, at 588–589, 592, 595–597; Walton, *supra* note 103, at 1513.

[157] Crootof, *supra* note *supra* note 103, at 608–609; Gross, *supra* note 78, at 484; Takano, *supra* note 110, at 6–7. See also US Department of Defense Cyber Strategy (2015), at 5, available at https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.

[158] ILC, Draft Articles on Prevention, *supra* note 21, at 152, Commentary to art. 2, para. 4 (emphases in the original).

probability of occurrence of an accident and the magnitude of its injurious impact'.[159] Thus, it covers activities carrying a 'low probability of causing disastrous harm', as well as operations where there is 'a high probability of causing significant harm'.[160] In cyberspace, this could potentially include physical, functional or non-physical harm to hardware, software, data or their individual users. Such harms may be caused by online mis- and disinformation campaigns, especially those taking place during elections[161] or public health crises,[162] as well as the exploitation of vulnerabilities in widely used IT supply chain products.[163] The determination of what amounts to significant harm involves a subjective assessment that varies depending on the circumstances prevailing at the time, in particular, existing scientific knowledge, the economic value of the activity or good in question and the extent of the damage caused.[164]

3 *Knowledge Requirement*

Both the no-harm and the Corfu Channel principles are triggered by actual or constructive knowledge of a risk and exclude unforeseeable harms.[165] However, the no-harm principle also applies where there is 'low probability' of 'disastrous harm'.[166] Thus, it may require more proactive measures of vigilance or monitoring,[167] variable on the basis of the seriousness of the harm.[168] Again, a requirement to be continuously vigilant in the use of ICTs[169] – or any other technology for that matter – depends on each state's capacity to act[170] and must be consistent with other international obligations. All in all, the more feasible it is for states to predict that a certain harmful

[159] *Ibid.*, para. 2.

[160] *Ibid.*, para. 3.

[161] See Sander, *supra* note 88, at 49–50.

[162] See Milanovic and Schmitt, *supra* note 72. See also Robinson and Spring, 'Coronavirus: How Bad Information Goes Viral', BBC (2020), available at www.bbc.co.uk/news/blogs-trending-51931394; Rankin, 'Russian media "spreading Covid-19 disinformation"', *Guardian* (2020), available at www.theguardian.com/world/2020/mar/18/russian-media-spreading-covid-19-disinformation. See also Committee on Economic, Social and Cultural Rights (CESCR), General Comment No. 14: The Right to the Highest Attainable Standard of Health (Article 12), E/C.12/2000/4, 11 August 2000, § 34. On due diligence obligations applying in relation to COVID-19, see Coco and de Souza Dias, 'Prevent, Respond, Cooperate: States' Due Diligence Duties vis-à-vis the Covid-19 Pandemic', 11 *Journal of Humanitarian Legal Studies* (2020) 218.

[163] See, e.g., reports on the widespread impact of the SolarWinds Hack: Sanger, Perlroth and Barnes, 'As Understanding of Russian Hacking Grows, So Does Alarm', *New York Times*, 2 January 2021, available at https://nyti.ms/3hvBUfA.

[164] ILC, Draft Articles on Prevention, *supra* note 21, at 153, Commentary to art. 2, para. 7.

[165] *Ibid.*, at 153 and 155, Commentary to art. 3, paras 5 and 18.

[166] *Ibid.*, at 152, Commentary to art. 2, para. 3.

[167] *Ibid.*, at 156, art. 5 and Commentary.

[168] *Ibid.*, at 154–155, Commentary to art. 3, paras 11 and 18; ILA Study, *supra* note 14, at 12; *Responsibilities and Obligations of States with Respect to Activities in the Area*, Advisory Opinion, 1 February 2011, ITLOS Reports (2011) 10, para. 117; Koivurova, *supra* note 9, para. 17.

[169] In defence of a duty to continuously monitor cyberspace, see Geiss and Lahmann, *supra* note 49, at 254–255, citing *Pulp Mills*, Judgment, 20 April 2010, ICJ Reports (2010), para. 197; Buchan, *supra* note 1, at 441–442; Bannelier-Christakis, *supra* note 78, at 30–31; Takano, *supra* note 110, at 7–8.

[170] See Buchan, *supra* note 1, at 441; Gross, *supra* note 78, at 503.

cyber operation is forthcoming, the greater the degree of diligence required. Such flexibility, however, must always be assessed against a core component of the no-harm principle, i.e. a state's duty to 'keep abreast of technological changes and scientific developments',[171] which suggests a requirement to continuously engage in capacity building, to the extent feasible in the circumstances.[172]

4 Legal Consequences

As seen earlier, the Corfu Channel principle is triggered once a state knows or should have known of the serious risk of an act contrary to the rights of other states emanating from or crossing its territory and is breached when the act in question occurs. It is at this point that the responsibility of the duty-bearer is engaged and other states can respond with countermeasures. Conversely, under the no-harm principle, the occurrence of harm or the risk thereof, which a state has failed to prevent or halt, does not automatically engage the responsibility of the duty-bearer. It is only after a state fails to compensate the victim for the damage caused that a breach of the no-harm principle arises.[173]

In this way, the no-harm principle is simultaneously a primary and secondary rule of international law: it requires states to take action and foresees the very consequences arising from a failure to act.[174] Those consequences are, first, *liability* for the harm caused, and, secondly, *responsibility* for the eventual failure to redress it.[175] This norm structure is a logical consequence of the principle's emphasis on reparation: states are given an opportunity to redress the harm before their responsibility is engaged. It is not the harm itself or the failure to prevent it that are unlawful,[176] but the failure to *redress* it. The advantages of applying this regime to cyberspace include increasing the costs of harmful cyber operations and deterring them, avoiding the stigma and antagonism associated with unlawful acts and fostering victim redress.[177] In the ICT context, given the interconnectivity and interdependence of different networks, international cooperation,[178] vulnerability disclosure[179] and cyber incident recovery plans[180] have been highlighted as key measures of redress.

[171] ILC, Draft Articles on Prevention, *supra* note 21, at 154 Commentary to art. 3, para. 11.

[172] States seem to be adamant about the need for capacity building. For recent practice, see Canada's Implementation of the 2015 GGE Norms, *supra* note 114, at 5; UK Multi-Stakeholder Advisory Group on Cyber Issues, 'Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015', at 5, available at www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf (last visited 10 June 2021).

[173] See Crootof, *supra* note 103, at 603; Walton, *supra* note 103, at 1487–1488; Sander, *supra* note 88, at 51; Dörr, *supra* note 78, at 96.

[174] Walton, *supra* note 103, at 1486–1487; Sander, *supra* note 88, at 50.

[175] ILC, Draft Articles on Prevention, *supra* note 21, at 148, General Commentary, para. 1; at 150, Commentary to art. 1, para. 6. See also Walton, *supra* note 103, at 1486–1488; Sander, *supra* note 88, at 51.

[176] See ILC, Draft Articles on Prevention, *supra* note 21, at 154, Commentary to art. 3, para. 7.

[177] Crootof, *supra* note 103, at 597–599, 604–608, 614; Walton, *supra* note 103, at 1511–1516.

[178] Stratégie internationale de la France pour le numérique, at 32, available at www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf (last visited 10 July 2021).

[179] G7, 'Cyber Norm Initiative: Synthesis of Lessons Learned and Best Practices', 26 August 2019, at 3, available at www.diplomatie.gouv.fr/IMG/pdf/_eng_synthesis_cyber_norm_initiative_cle44136e.pdf.

[180] UK Network and Information Systems Regulations 2018, *supra* note 113, pt. 2.

C *The Obligation to Protect Human Rights Online*

The increasing number of everyday activities which are carried out online has exposed human rights to infinite possibilities of harm. Just to mention probably the most egregious example, the right to privacy is seriously endangered by the constant tracking and mining of online activities and data, as well as their subsequent profiling. Likewise, the rights to freedom of thought, information and expression may be undermined by online disinformation campaigns, the proliferation of fake news or censorship. Cyber-bulling, defamation and hate speech can spread incredibly quickly, with detrimental effects on individuals' rights and reputation.[181]

International human rights law (IHRL) imposes on states a set of protective obligations against these harms. They cover online activities to the extent that they take place under a state's jurisdiction.[182] In the cyber realm as in any other area of human activity, states not only have a 'negative' duty to *respect* human rights online – i.e. not to violate those rights with their own actions. They also have a positive duty to adopt all reasonable measures to *protect* the human rights of persons under their jurisdiction against threats posed by other entities, be them foreign governments, companies, criminals or other actors.[183] In addition, states must *ensure* the effective enjoyment of human rights on the Internet.[184] Positive obligations to protect and ensure may be potentially identified for all human rights.[185] With specific reference to the rights which are more commonly endangered online, one may highlight the rights to privacy,[186] honour and reputation,[187] and freedom of information and expression.[188]

[181] ECtHR, *Delfi v. Estonia*, Appl. no. 64569/09, Judgment of 16 June 2015, para. 110.

[182] UN GGE Report 2015, *supra* note 5, § 28(b).

[183] ECtHR, *Bărbulescu v. Romania*, Appl. no. 61496/08, Judgment of 12 January 2016, para. 110, with respect to the right to privacy. In this sense, see also Milanovic and Schmitt, *supra* note 72, at 270ff.

[184] Cf. HRComm, General Comment No. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant, UN Doc CCPR/C/21/Rev.1/Add.13, 26 May 2004, § 8. See also HRComm, CESCR General Comment No. 3: The Nature of States Parties' Obligations (Article 2(1) of the Covenant), E/1991/23, 14 December 1990, § 1; IACtHR, *Velasquez Rodriguez v. Honduras*, Judgment (Merits), 29 July 1988, paras 166–167.

[185] See, e.g., International Covenant on Civil and Political Rights 1966, 999 UNTS 171, art. 2(1)–(2) (hereinafter 'ICCPR'); International Covenant on Economic, Social and Cultural Rights 1966, 993 UNTS 3, art. 2(1) (hereinafter 'ICESCR'); American Convention on Human Rights 1978, OAS Treaty Series No. 36, 1144 UNTS 123, art. 1(1) (hereinafter 'ACHR'); European Convention for the Protection of Human Rights and Fundamental Freedoms, 1953, 213 UNTS 221, art. 1 (hereinafter 'ECHR').

[186] ECtHR, *X and Y v. the Netherlands*, Appl. no. 8978/80, Judgment of 26 March 1985, para. 23; ECtHR, *Bărbulescu v. Romania*, Appl. no. 61496/08, Judgment of 12 January 2016, para. 108; ECtHR, *Hämäläinen v. Finland*, Appl. no. 37359/09, Judgment of 16 July 2014, para. 62; ECtHR, *Nicolae Virgiliu Tănase v. Romania*, Appl. no. 41720/13, Judgment of 25 June 2019, para. 125. Cf. also HRComm, CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, UN Doc. HRI/GEN/1/Rev.9, 8 April 1988, § 10.

[187] HRComm, General Comment No. 16, *supra* note 186, §§ 1 and 11. The principles established therein, even though not referred to ICTs specifically, are in principle applicable to such technologies as well.

[188] HRComm, General Comment No. 34, Article 19: Freedoms of opinion and expression, UN Doc CCPR/C/GC/34, 12 September 2011, §§ 12, 15.

Due diligence, in this context, designates the standard of conduct that states must meet to comply with the said positive obligations.[189] Notably, positive human rights duties are owed not only to states but also individuals and the international community as a whole. They require states to prevent threats to the enjoyment of human rights, halt harms once they have initiated and remedy their effects, to the extent possible.[190] Attribution of the harmful conduct is unnecessary: all that must be demonstrated is that the state failed to adopt the necessary and reasonable protective measures, irrespective of who or what caused the harm.[191]

Such measures may vary greatly depending on the human right in question, the type of threat and/or harm which the state is trying to prevent and the circumstances prevailing at the time. Treaty bodies have adopted relatively open-ended formulas when it comes to compliance. For instance, states have been urged to establish an adequate legal framework[192] providing for the availability of civil remedies and criminal provisions enabling effective investigations and prosecutions of rights violations.[193] Such laws should cover, inter alia, the prohibition of online speech constituting incitement to hatred, discrimination or violence based on certain characteristics, content moderation mechanisms, educational campaigns, the prohibition of Internet shutdowns and arbitrary content takedowns,[194] as well as corporate responsibility, public–private partnerships and export control of IT products.[195]

States' positive human rights obligations containing a due diligence standard must not be confused with the related concept of corporate 'human rights due diligence', i.e. the non-binding responsibility of businesses to mitigate the human rights impact of their activities.[196] That said, states themselves have a positive obligation to establish

[189] HRComm, General Comment No. 31, *supra* note 184, § 8; Besson, *supra* note 39, at 2, 4–5; Milanovic and Schmitt, *supra* note 72, at 270ff.

[190] With respect to civil and political rights, see HRComm, General Comment No. 31, *supra* note 184, §§ 8, 17; for economic, social and cultural rights, see, e.g., CESCR, General Comment No. 24 on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities, UN Doc E/C.12/GC/24, 10 August 2017, § 14.

[191] Seibert-Fohr, 'From Complicity to Due Diligence: When Do States Incur Responsibility for Their Involvement in Serious International Wrongdoing?', 60 *GYIL* (2017) 667, at 670; Keller and Walther, 'Evasion of the International Law of State Responsibility? The ECtHR's Jurisprudence on Positive and Preventive Obligations under Article 3', *International Journal of Human Rights* (2019) 1, at 3; HRComm, General Comment No. 31, *supra* note 184, § 8.

[192] *Bărbulescu v. Romania*, Appl. no. 61496/08, Judgment of 12 January 2016, paras 115–116; HRComm, General Comment No. 31, *supra* note 184, §§ 7, 13; HRComm, General Comment No. 36, *supra* note 43, §§ 4, 13, 22.

[193] ECtHR, *Nicolae Virgiliu Tănase v. Romania*, Appl. no. 41720/13, Judgment of 25 June 2019, para. 127; HRComm, General Comment No. 31, *supra* note 184, §§ 8, 18; HRComm, General Comment No. 36, *supra* note 43, §§ 13, 19, 27–28.

[194] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/74/486, 9 October 2019, §§ 29, 34, 40–55, 57(b).

[195] Human Rights Council, Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/41/35, 28 May 2019, §§ 15–20, 29–38.

[196] On this principle, see Bonnitcha and McCorquodale, 'The Concept of "Due Diligence" in the UN Guiding Principles on Business and Human Rights', 28 *European Journal of International Law* (*EJIL*) (2017) 899; Ruggie and Sherman, 'The Concept of "Due Diligence" in the UN Guiding Principles on Business and Human Rights: A Reply to Jonathan Bonnitcha and Robert McCorquodale', 28 *EJIL* (2017) 921.

a legal framework that requires businesses to, in turn, exercise their own due diligence.[197] This is all the more important in the cyber context, since the Internet and other ICTs are mostly owned, controlled or designed by private entities.[198]

While states' protective duties under IHRL are also subject to a requirement of capacity to act, common to other due diligence obligations,[199] they may be 'substantively … more demanding' than those deriving from general international law, often including duties to actively seek knowledge of violations.[200] Other distinctive features include jurisdictional triggers (Section 4.C.1); the type of harms covered (Section 4.C.2); the knowledge requirement (Section 4.C.3); as well as the legal consequences of a failure to protect applicable human rights (Section 4.C.4).

1 *State Jurisdiction*

Under some IHRL treaties, before states' positive obligations in respect of online or offline harms can be triggered, jurisdiction must be established.[201] In IHRL, the concept of jurisdiction includes not only the territory of the duty-bearer but also effective control over certain physical spaces, persons or events located extraterritorially. Considering the multi-layered and transnational nature of cyberspace, comprising physical infrastructure, logical systems, data and human activity across multiple boundaries,[202] extraterritorial models of jurisdiction are particularly relevant in the context of states' protective obligations under IHRL.

First, there is broad agreement that extraterritorial jurisdiction 'follows' individuals wherever a state exercises some form of physical control or authority over them.[203] This is what is known as the 'personal' model of extraterritorial jurisdiction and most human rights bodies[204] and commentators[205] agree that it applies to both negative and positive human rights obligations. Secondly, although not without contestation,[206]

[197] CESCR, General Comment No. 24, *supra* note 190, §§ 16–18, with respect to economic, social and cultural rights, but with a principle that could be extended to civil and political rights as well; Besson, *supra* note 39, at 8.

[198] Smith, 'A Moment of Reckoning: The Need for a Strong and Global Cybersecurity Response', *Microsoft on the Issues*, 17 December 2020, available at https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/.

[199] Besson, *supra* note 39, at 5–7.

[200] Milanovic and Schmitt, *supra* note 72, at 281–282, citing as an example CESCR, General Comment No. 24, *supra* note 190, § 33.

[201] See, e.g., ICCPR, *supra* not 184, art. 2(1); ECHR, *supra* not 184, art. 1; ACHR, *supra* not 184, art. 1(1).

[202] Sullivan, *supra* note 3, at 454 n.88.

[203] HRComm, General Comment No. 31, *supra* note 184, § 10.

[204] See, e.g., Inter-American Commission on Human Rights (IAComHR), *Coard et al. v. United States*, Report No. 109/99, 29 September 1999, para. 37; ECtHR, *Al-Skeini and others v. United Kingdom*, Appl. no 55721/07, Judgment of 7 July 2011, paras 136–139.

[205] Milanovic, *supra* note 147, at 119. But the ECtHR has been reluctant to recognize this model in relation to extraterritorial kinetic force in the absence of governmental control (see ECtHR, *Banković and others v. Belgium and others*, Appl. no 52207/99, Decision of 12 December 2001, paras 74–82; ECtHR, *Al-Skeini and others v. United Kingdom*, Appl. no 55721/07, Judgment of 7 July 2011, paras 136–137). For a recent analysis, see Milanovic, 'The Murder of Jamal Khashoggi: Immunities, Inviolability and the Human Right to Life', 20 *Human Rights Law Review* (2020) 1, at 23–24.

[206] See Besson, *supra* note 39.

several human rights bodies have expressed the vew that jurisdiction may also be extended extraterritorially to the reasonably foreseeable human rights impact of the activities of entities, such as companies, which are incorporated or located in the duty-bearer's territory, or otherwise subject to a state's effective control.[207] Thirdly, the Human Rights Committee has advanced a more expansive, 'functional' approach to extraterritorial jurisdiction, grounded in the exercise of control over the *enjoyment* of the rights in question, regardless of any *physical* control over territory, the perpetrators or the individual victim.[208]

Arguably, the functional approach to jurisdiction is best suited to address contemporary forms of effective control gained remotely through ICTs over victims, perpetrators and events.[209] Thus, its appeal resides in the increased protection of human rights, whose exercise increasingly depends on online systems. But while the functional model has received some support in respect of *negative* human rights duties,[210] many oppose its applicability to *positive* human rights obligations, fearing the lack of necessary government powers beyond a state's territory or spatial control.[211] Nevertheless, the practical impact of this jurisdictional model should not be overstated: any protective obligation only extends insofar as the duty-bearer has the capacity to adopt the necessary measures in question.[212] Capacity, in this context, includes the ability to influence the behaviour of the perpetrators,[213] or to predict events, the availability of

[207] HRComm, General Comment No. 36, *supra* note 43, § 22, with respect to the right to life; CESCR, General Comment No. 14, *supra* note 162, § 39; CESCR, General Comment No. 15: The Right to Water (Articles 11 and 12 of the Covenant), UN Doc E/C.12/2002/11, 20 January 2003, § 33; CESCR, Statement on the Obligations of States parties regarding the corporate sector and economic social and cultural rights, UN Doc E/C.12/2011/1, 20 May 2011, § 5; IACtHR, Advisory Opinion OC-23/17, Requested by the Republic of Colombia: The Environment and Human Rights, 15 November 2017, paras 101–102. See also Milanovic and Schmitt, *supra* note 72, at 264–265. Although this model of jurisdiction may overlap with the requirement of a state's capacity to act, the two are grounded in different criteria and underlying rationales. Jurisdiction captures the connection between the state and the protected human right on the basis of effective control over different aspects of this connection. Conversely, capacity to act limits a state's protective obligations on the basis of a range of factors, including control over the activities or perpetrators in question, or a less demanding ability to influence their behaviour. See *contra* Besson, *supra* note 39, at 2.

[208] HRComm, General Comment No. 36, *supra* note 43, § 63.

[209] See Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law', 7 *Law & Ethics of Human Rights* (2013) 47.

[210] Milanovic, *supra* note 147, at 209; Goodman, Heyns and Shany, 'Human Rights, Deprivation of Life and National Security: Q&A with Christof Heyns and Yuval Shany on General Comment 36' (2019), at 1–2, available at www.justsecurity.org/62467/human-life-national-security-qa-christof-heyns-yuval-shany-general-comment-36/; *Sergio Euben Lopez Burgos v. Uruguay*, Human Rights Committee (HRComm) Communication No. 52/1979, UN Doc. CCPR/C/13/D/52/1979, 29 July 1981, § 12.3; *Lilian Celiberti de Casariego v. Uruguay*, HRComm Communication No 56/1979, UN Doc. CCPR/C/13/D/56/1979, 29 July 1981, § 10.3; ECtHR, *Issa and Others v. Turkey*, Appl. no. 31821/96, Judgment of 16 November 2004, § 71.

[211] See, e.g., the account of the debate in Milanovic, *supra* note 205, at 19–20; and Milanovic, *supra* note 147, at 209, 210–212, 219–220.

[212] For example, the ICESCR, *supra* note 184, has no express jurisdictional threshold and yet most of its obligations are positive ones, i.e. duties to protect and ensure social, economic and cultural human rights.

[213] *Bosnian Genocide*, Judgment, 26 February 2007, ICJ Reports 2007, para. 430.

resources and the duty to respect and protect other human rights.[214] Of course, there is a difference between a state having no jurisdiction at all and it being incapable of protecting human rights within its jurisdiction: in the latter case, the state's capacity to act, along with other elements of the obligation, must still be assessed. Yet, states are not required to do the impossible or to discharge a 'disproportionate burden'[215] but are expected to adopt measures that are reasonable in the circumstances.[216] Thus, as in any other jurisdictional model, the requirement of capacity to act overlaps with and modulates a state's functional jurisdiction over human rights online.[217]

2 *Type of Harm*

Protective obligations under IHRL cover a wide spectrum of harms, including any conduct by public or private entities that impairs the enjoyment of human rights online or offline, such as privacy and freedom of expression. Unlike the no-harm principle, the online harm in question need not have a transboundary nature: provided jurisdiction is established, a state must protect human rights regardless of the harm's origin or trajectory.

3 *Knowledge Requirement*

Given the multitude of threats to human rights, it would be unrealistic and unreasonable to expect a state to be in a position to adopt protective measures against any such threats. Rather, states are only capable and thus required to act in the presence of some level of knowledge that there is a risk to human rights. With respect to the right to life, the Human Rights Committee and the Inter-American Court of Human Rights have stressed the requirement of reasonable foreseeability of threats[218] and constructive knowledge of an immediate and certain risk,[219] respectively. Whilst these pronouncements were concerned with the protection of the right to life, there is no particular reason not to extend them to positive obligations to protect other human rights, including in cyberspace. This means that, under IHRL, states must also exercise due diligence in actively seeking and evaluating available information about threats to human rights under their jurisdiction.[220]

[214] Cf. ECtHR, *Osman v. United Kingdom*, Appl. no. 87/1997/871/1083, Judgment of 28 October 1998, para. 116.

[215] *Ibid.*; see also ECtHR, *Nicolae Virgiliu Tănase v. Romania*, Appl. no. 41720/13, Judgment of 25 June 2019, para. 136.

[216] ECtHR, *McCann and Others v. United Kingdom*, Appl. no. 19009/04, Judgment of 27 September 1995, para. 151; *Velasquez Rodriguez v. Honduras*, Judgment (Merits), 29 July 1988, para. 167. See also The Netherlands, Letter of 5 July 2019, *supra* note 62, Appendix, at 4; Comments by Member States on the initial pre-draft of the OEWG report: Republic of Korea, *supra* note 47, at 5.

[217] Besson, *supra* note 39, at 5.

[218] As, for instance, affirmed by the HRC with respect to the right to life. See HRComm, General Comment No. 36, *supra* note 43, § 21; cf. also ECtHR, *Osman v. United Kingdom*, App. No. 87/1997/871/1083, Judgment of 28 October 1998, paras 115–116.

[219] IACtHR, *Sawhoyamaxa Indigenous Community v. Paraguay*, Judgment (Merits, Reparations and Costs), 29 March 2006, § 155; cf. very similar language in ECtHR, *Nicolae Virgiliu Tănase v. Romania*, Appl. no. 41720/13, Judgment of 25 June 2019, para. 136.

[220] HRComm, General Comment No. 36, *supra* note 43, §§ 13, 23, 27.

4 *Legal Consequences of a Failure to Protect Human Rights*

Unlike the Corfu Channel and the no-harm principles, positive obligations to protect and ensure human rights are breached by the mere lack of diligence, i.e. the wrongful omission or inaction in adopting the required measures.[221] This is true to the extent that states must prevent objectively foreseeable *threats* to human rights.[222] As such, the mere emergence of a risk of harm, regardless of whether or not it materializes, may breach positive human rights obligations.[223] Although the actual occurrence of the prohibited harm is generally indicative that the state has failed to exercise due diligence, proof of causation between the lack of diligence and the harm is unnecessary. According to the ECtHR, a state's knowledge of, acquiescence in or connivance to human rights violations perpetrated by third parties suffices to demonstrate a breach of that state's positive duties to protect those rights.[224]

Importantly, a breach of positive human rights obligations arises not only from complete inaction but also from the adoption of insufficient or ineffective measures, when more appropriate ones were available.[225] Conversely, the occurrence of the prohibited harm does not necessarily mean that the state violated its due diligence obligations under IHRL. A violation only arises if it is proven that the state failed to adopt protective measures that it could have reasonably implemented.[226]

D *Cyber Due Diligence in International Humanitarian Law*

Cyber operations are by now part and parcel of modern warfare. Whilst they may specifically target military infrastructure, cyber weapons and tactics have the potential to

[221] See, e.g., *ibid.*, § 7.

[222] Todeschini, 'The Human Rights Committee's General Comment No. 36 and the Right to Life in Armed Conflict', *OpinioJuris* (21 January 2019), available at http://opiniojuris.org/2019/01/21/the-human-rights-committees-general-comment-no-36-and-the-right-to-life-in-armed-conflict/.

[223] This principle applies at the very least to the right to life and the right not to be subjected to torture and ill-treatment (see, e.g., HRComm, General Comment No. 36, *supra* note 43, § 7; ECtHR, *Keller v. Russia*, Appl. no. 26824/04, Judgment of 17 October 2013, para. 82; ECtHR, *Osman v. United Kingdom*, Appl. no. 87/1997/871/1083, Judgment of 28 October 1998, para. 116; ECtHR, *O'Keeffe v. Ireland*, Appl. no. 35810/09, Judgment of 28 January 2014, paras 16, 162; ECtHR, *Kurt v. Turkey*, Appl. no. 15/1997/799/1002, Judgment of 25 May 1998, para. 69. It also seems to apply to the right to non-discrimination, including in the context of online hate speech (see Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc A/74/486, 9 October 2019, §§ 13, 14(f), 16). See, generally, Stoyanova, 'Fault, Knowledge and Risk Within the Framework of Positive Obligations Under the European Convention on Human Rights', 33 *Leiden Journal of International Law* 601 (2020).

[224] See European Commission of Human rights (ECommHR), *Yaşa v. Turkey*, Appl. no. 22495/93, Report, 8 April 1997, paras 106–107; ECtHR, *Özgür Gündem v. Turkey*, Appl. no. 23144/93, 16 March 2000, paras 38–46; ECtHR, *Kılıç v. Turkey*, Appl. no. 22492/93, Judgment of 28 March 2000, paras 57, 64, 68; EctHR, *Mahmut Kaya v. Turkey*, Appl. no. 22535/93, Judgment, 28 March 2000, paras 74, 80, 85–92. All these cases are discussed in Milanovic, 'State Acquiescence or Connivance in the Wrongful Conduct of Third Parties in the Jurisprudence of the European Court of Human Rights' (15 September 2019), at 3–6, available at https://ssrn.com/abstract=3454007.

[225] Cf. ECtHR, *Hatton v. UK*, Appl. no. 36022/97, Judgment of 8 July 2003, paras 138–142.

[226] Cf. ECtHR, *E. and others v UK*, Appl. no. 33218/96, Judgment of 26 November 2002, paras 99–100.

intentionally or indiscriminately[227] disable civilian infrastructure and disrupt the provision of services essential to the civilian population. Many states[228] and most commentators agree that, at the very least, cyber operations having kinetic effects similar to those of traditional uses of armed force – for example, the destruction of civilian objects or harm to civilians – are covered by the provisions of IHL when carried out during an armed conflict.[229] But it remains unclear whether, in the absence of physical damage, the mere corruption of data or functional system disruptions amount to attacks governed by IHL.[230]

Numerous rules of IHL establish protective obligations requiring states to exercise due diligence.[231] Of particular relevance to ICTs are the obligations to ensure respect for IHL, including by third parties (Section 4.D.1), and adopt defensive precautions to avoid or minimize harm to civilian objects and the civilian population (Section 4.D.2).

1 *The General Duty to Ensure Respect for International Humanitarian Law in Cyberspace*

A protective obligation is codified in Article 1 common to the 1949 Geneva Conventions on the Protection of Victims of War, which requires states to respect and *ensure respect* for the provisions of the conventions[232] – a provision repeated almost *verbatim* in Article 1(1) of Additional Protocol I.[233] The customary status of this rule was recognized by the ICJ, as well as its application to both international and non-international armed conflict.[234] Given the *erga omnes* nature of IHL, not only parties

[227] ICRC, Position Paper, 'International Humanitarian Law and Cyber Operations during Armed Conflicts' (2019), at 5, available at www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.

[228] See, e.g., Jeremy Wright, UK Attorney General's Office, Speech, 'Cyber and International Law in the 21st Century' (23 May 2018), available at www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century; Comments by Member States on the Initial Pre-Draft of the OEWG Report: United States, *supra* note 47, at 2; Juul, *supra* note 2.

[229] See, e.g., *Tallinn Manual 2.0*, *supra* note 6, rule 82, para. 16; *Nuclear Weapons*, Advisory Opinion, 8 July 1996, ICJ Reports (1996), para. 86. See also Durham, 'Cyber Operations During Armed Conflict: 7 Essential Law and Policy Questions', *Humanitarian Law & Policyt* (26 March 2020), available at https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/.

[230] See Rödenhauser, 'Hacking Humanitarians? IHL and the Protection of Humanitarian Organizations Against Cyber Operations', *EJIL: Talk!* (16 March 2020), available at www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyber-operations/.

[231] See Longobardo, 'The Relevance of the Concept of Due Diligence for International Humanitarian Law', 37 *Wisconsin International Law Journal* (2020) 44; and Berkes, 'The Standard of "Due Diligence" as a Result of Interchange between the Law of Armed Conflict and General International Law', 23 *Journal of Conflict & Security Law* (2018) 433.

[232] Article 1 common to: Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field 1949, 75 UNTS 31; Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea 1949, 75 UNTS 85; Geneva Convention (III) relative to the Treatment of Prisoners of War 1949, 75 UNTS 135; Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War, 75 UNTS 287.

[233] Additional Protocol I, *supra* note 44, art. 1(1).

[234] *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States)*, Judgment, 27 June 1986, ICJ Reports (1987) 14, para. 220; ICRC, *Commentary on the First Geneva Convention* (2016), art. 1 ('Respect for the Convention'), paras 125–126, available at https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=72239588AFA66200C1257F7D00367DBD (hereinafter '*2016 Commentary*').

to an armed conflict but all states are bound to do 'everything in their power to ensure that the humanitarian principles underlying the Conventions are applied universally'.[235] According to Rule 144 of the International Committee of the Red Cross's (ICRC) Customary IHL Study,[236] this obligation requires States not only to refrain from committing or encouraging violations of IHL[237] but also to take positive steps to ensure – even in peacetime[238] – that other entities comply with IHL.[239]

This obligation also applies in cyberspace and entails a duty to act, as far as possible, to prevent and halt cyber operations constituting violations of IHL. Its broad scope of application covers potential violations by state agents, as well as private entities over which a state exercises authority, such as populations under belligerent occupation,[240] or exerts a reasonable degree of influence, including other states and non-state groups located in different parts of the world.[241]

As with other protective obligations, the duty to respect and ensure respect for IHL is triggered and limited by a state's capacity to act.[242] This, in turn, depends on a range of factors, such as available resources, the gravity of the violation and the degree of control or influence that the state exercises over the direct perpetrators.[243] Yet lack of military, economic or other resources does not exempt states from what remains a binding legal obligation to acquire and employ all reasonable means to ensure respect for IHL, including in cyberspace.[244] The duty is triggered not only by a state's knowledge of violations but also by objective foreseeability.[245] However, though it *arises* from

[235] ICRC, *Geneva Convention Relative to the Protection of Civilian Persons in Time of War: Commentary* (1958), at 16; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 9 July 2004, ICJ Reports (2004) 136, paras 158–159.

[236] J.-M. Henckaerts and L. Doswald-Beck (eds), *Customary International Law.* Volume 1: *Rules* (2009), at 509–513. Rule 139, instead, reproduces verbatim the language of common Article 1, but it limits its scope of application to armed forces and other entities acting on the instructions, or under the direction or control of a party to the conflict. See *ibid.*, at 495ff.

[237] ICRC, *2016 Commentary*, *supra* note 234, paras 154. 158–163.

[238] *Ibid.*, paras 127–128 and 185.

[239] *Ibid.*, paras 121, 153–154, 164–173. On this obligation generally, see Dörmann and Serralvo, 'Common Article 1 to the Geneva Conventions and the Obligation to Prevent International Humanitarian Law Violations', 96 *International Review of the Red Cross* (*IRRC*) (2014) 707. See also Longobardo, *supra* note 231, at 57–60; and Berkes, *supra* note 231, at 442. See *contra*, see Zych, 'The Scope of the Obligation to Respect and to Ensure Respect for International Humanitarian Law', 27 *Windsor Yearbook of Access to Justice* (2009) 251; Robson, 'The Common Approach to Article 1: The Scope of Each State's Obligation to Ensure Respect for the Geneva Conventions', 25 *Journal of Conflict and Security Law* (2020) 101. On examples of operational measures, see European Union, Updated European Union Guidelines on Promoting Compliance with International Humanitarian Law, 2009/C 303/06, 15 December 2009, § 16.

[240] ICRC, *2016 Commentary*, *supra* note 234, para. 150.

[241] *Ibid.*, paras 150, 153–154.

[242] *Ibid.*, paras 166, 187.

[243] *Ibid.*, paras 165–166 and, *mutatis mutandis*, *Bosnian Genocide*, Judgment, 26 February 2007, ICJ Reports 2007, para. 430. See also Longobardo, *supra* note 231, at 60–62.

[244] ICRC, *2016 Commentary*, *supra* note 234, para. 187.

[245] *Ibid.*, paras 150, 164.

the moment IHL violations become known or foreseeable, a breach only occurs if the actual harm materializes, like the Corfu Channel and no-harm principles.[246]

States may comply with this rule by simply adopting measures well-known in the law of state responsibility, such as invoking a breach of IHL by a third state through adjudicative or diplomatic means,[247] demanding its cessation, guarantees of non-repetition or reparations,[248] refraining from recognizing the situation as lawful and rendering assistance to the state in breach,[249] as well as taking effective steps to investigate and redress the violations.[250]

2 *The Duty to Adopt Protective Precautions against the Effects of Cyber Warfare*

The principle of precaution enshrined in several IHL provisions also embodies a set of protective duties. Article 51 of Additional Protocol I generally provides that '[t]he civilian population and individual civilians shall enjoy general protection against dangers arising from military operations'.[251] It is immediately evident how cyber warfare may pose a challenge to the application of such rule. To begin with, civilian cyber-infrastructures may not be easily distinguishable from lawful military objectives, as these often depend on services and resources provided by private entities.[252] The interconnectivity of cyberspace may also mean that cyberattacks directed against military objectives may spill over into civilian systems, causing disruption or loss of functionality.[253]

To obviate such undesirable results, Article 58 of Additional Protocol I requires parties to a conflict to adopt precautionary measures to protect civilian populations and objects against the effects of attacks, provided they exercise control over the territory, physical infrastructure or, in our view, the operational systems which may be targeted.[254] The rule has achieved customary status, as recognized by Rules 22–24 of the ICRC's Study on Customary IHL, and is applicable not only in international armed conflict but also, arguably, in non-international ones.[255]

[246] ICRC, *2016 Commentary*, *supra* note 234, para. 166 establishes a parallelism between common Article 1 to the Geneva Conventions, *supra* note 231, and Genocide Convention, *supra* note 31, art. 1. The ICJ in *Bosnian Genocide*, Judgment, 26 February 2007, ICJ Reports 2007, para. 431, established that a breach of the duty to prevent occurs only if genocide is actually committed, in line with ARSIWA, *supra* note 20, art. 14(3).

[247] ICRC, *2016 Commentary*, *supra* note 234, para. 181.

[248] ARSIWA, *supra* note 20, art 48. Cf. ICRC, Memorandum to the States Parties to the Geneva Conventions of 12 August 1949 concerning the conflict between Islamic Republic of Iran and Republic of Iraq (1983), available at https://casebook.icrc.org/case-study/icrc-iraniraq-memoranda.

[249] ARSIWA, *supra* note 20, arts. 16, 40–41; cf. ICRC, *2016 Commentary*, *supra* note 234, paras 158–163.

[250] Koivurova, *supra* note 9, para. 32.

[251] Additional Protocol I, *supra* note 44, art. 51. See generally Jensen, 'Precautions against the Effects of Attacks in Urban Areas', 98 *IRRC* (2016) 147; Quéguiner, 'Precautions under the Law Governing the Conduct of Hostilities', 88 *IRRC* (2006) 793.

[252] Cf. Additional Protocol I, *supra* note 44, art. 52(2).

[253] See Gisel and Rodenhäuser, *Cyber Operations and International Humanitarian Law: Five Key Points* (2019) available at https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/.

[254] Sandoz, Swinarski and Zimmermann, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (1987), at 692, para. 2239.

[255] Henckaerts and Doswald-Beck, *supra* note 236, at 69–70.

Along with other protective obligations, the duty to adopt precautions against the effects of attacks is triggered and limited by a state's capacity to act, only covering measures that are 'practicable or practically possible'.[256] In respect of cyberattacks, this might require states to adopt, to the extent feasible, measures such as establishing a clear separation between military and civilian cyberinfrastructure and networks, identifying and protecting critical civilian infrastructure and services – such as those related to the provision of medical assistance, electricity, telecommunications, transport and distribution of objects indispensable for the survival of civilians – from potentially disruptive cyber operations, such as by taking them offline.[257]

5 Conclusion: A Patchwork of Primary Cyber Due Diligence Duties

Throughout this contribution, we have stressed that the concept of due diligence is best understood as a flexible standard of care or good governance found in a variety of primary rules of international law across a range of areas. Thus, in a way, there is a patchwork of different but overlapping protective obligations requiring diligent behaviour in cyberspace. Yet a set of core elements also threads them together.

First, all protective obligations surveyed above presuppose the exercise of state sovereignty, jurisdiction or some level of control over a territory, the right-holder, the perpetrator or the events in question.[258] Secondly, and relatedly, those obligations are subject to and limited by a state's capacity to act,[259] which gives effect to the idea that states have common but differentiated responsibilities in international law.[260] Thirdly, those flexible obligations of conduct are coupled with obligations of result to put in place the minimal legislative, judicial and executive infrastructure needed to exercise due diligence.[261] Fourthly, a state is only required to act in the presence of some degree of information about the harm or risk in question, ranging from actual or constructive knowledge to objective foreseeability.[262] Lastly, all these elements are geared towards a central duty to prevent, halt and/or redress harm or the risk thereof, consisting of an

[256] Cf., e.g., US Department of Defense, Law of War Manual (June 2015, updated December 2016), at 192, § 5.2.3.2.

[257] Cf. ICRC, *Position Paper*, *supra* note 227, at 6. See also Mačák, Gisel and Rodenhäuser, 'Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong Are International Law Protections?', *Just Security* (2020), available at www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/.

[258] ILA Study, *supra* note 14, at 5; HRComm, General Comment No. 36, *supra* note 43, § 22.

[259] *Alabama Claims (United States v UK)* (1872) 29 RIAA 125, *supra* note 15, at 129; *ILA Study*, *supra* note 14, at 20, 47; HRComm, General Comment No. 36, *supra* note 43, § 21; *Bosnian Genocide*, Judgment, 26 February 2007, ICJ Reports 2007, paras 430–432; *Nicaragua*, *supra* note 41, para. 157. See also Koivurova, *supra* note 9, paras 17, 19.

[260] Koivurova, *supra* note 9, para. 19.

[261] ILC, Draft Articles on Prevention, *supra* note 21, at 155–156, Commentary to art. 3, para. 17; art. 5 and Commentary; ILA Study, *supra* note 14, at 124; *Alabama Claims (United States v UK)* (1872) 29 RIAA 125, 131; Koivurova, *supra* note 9, para. 21; Pisillo-Mazzeschi, *supra* note 14, at 26–27; Kolb, *supra* note 37, at 117, 127; Couzigou, *supra* note 101, at 50–51; Okwori, *supra* note 50, at 223; Krieger & Peters, *supra* note 35.

[262] ILA Study, *supra* note 14, at 47.

act contrary to the rights of other states, significant transboundary harm or a violation of more specific international rules, such as IHRL and IHL.

These common threads raise the following question, foreshadowed at the beginning of this paper: is there a general principle of due diligence in international law? Perhaps. This is what the ICJ seemed to imply when, in *Pulp Mills*, it stated that 'the principle of prevention is a customary rule, and as such it has its origins in the [standard of] due diligence that is required of a State in its territory'.[263] In the same vein, citing the Alabama Claims arbitration, the *Trail Smelter* arbitral tribunal held that both arbitrations were decided on the basis of the 'same general principle' according to which '[a] State owes at all times a duty to protect other States against injurious acts by individuals from within its jurisdiction'.[264] The ILA[265] and some states have also supported this position, particularly in the context of cyberspace.[266] But whether or not this holds true, it should not detract from the fact that a comprehensive legal framework of *binding* protective obligations to prevent, halt and redress harm already applies in cyberspace, however patchy or fragmented it is.

Such framework comprises at least two different primary rules of general international law, namely the Corfu Channel and the no-harm principles. In addition, different obligations of due diligence arising under specialized branches of international law apply concurrently to cover different uses, aspects and consequences of ICTs. Among them, we have highlighted the positive obligation to protect human rights online, as well as the duty to ensure respect for IHL and to adopt precautions against the effects of cyberattacks in armed conflict.

While the said rules overlap and could be interpreted systematically, insofar as they work towards similar goals, they remain separate and should not be conflated. Each has different triggers, requirements and standards of care. It may well be that, from their similarities, one can derive a general principle of international law. Furthermore, states maintain the prerogative to develop – through conventional or customary international law – a new specialized duty containing a 'cyber due diligence' standard. This duty may well be modelled on any of the existing protective obligations or a mix thereof, mirroring Rule 6 of the Tallinn Manual. Yet, in debates about diligent state behaviour in cyberspace, doubts about a general principle or a cyber-specific protective obligation should not be presented as an alternative to a legal vacuum. For international law already provides more than meets the eye: a patchwork of protective duties that, together, require states to do their best to prevent, halt and respond to a wide range of online harms.

[263] *Pulp Mills*, Judgment, 20 April 2010, ICJ Reports (2010), para. 101 (emphasis added). See also ILA Study, *supra* note 14, at 6; Koivurova, *supra* note 9, para. 41; Couzigou, *supra* note 101, at 39; Hankinson, 'Due Diligence and the Gray Zones of International Cyberspace Laws', *Michigan Journal of International Law Blog* (November 2017), available at www.mjilonline.org/due-diligence-and-the-gray-zones-of-international-cyberspace-laws/.

[264] *Trail Smelter* (*United States v. Canada*) (1941) 3 RIAA 1911, at 1963, 1965.

[265] ILA Study, *supra* note 14, at 6.

[266] See, e.g., Comments by Member States on the initial pre-draft of the OEWG report, *supra* note 47, France (at 3), Republic of Korea (at 2, 5); 'International Law and Cyberspace: Finland's National Positions', at 4, available at https://bit.ly/3ecxSGR (last visited 10 July 2021).