CYBER OPERATIONS AND THE STATUS OF DUE DILIGENCE OBLIGATIONS IN INTERNATIONAL LAW

JACK KENNY

Research Fellow in International Law, British Institute of International and Comparative Law, London, UK
Email: j.kenny@biicl.org

Abstract This article adopts a critical approach towards scholarship seeking to identify binding due diligence obligations for States in cyberspace. The article demonstrates that due diligence obligations are anchored in specific primary rules and are not a universal standalone source from which it is possible to derive binding obligations for all areas of activity. The consensus position of States in United Nations fora clearly determines that due diligence in cyberspace is a voluntary, non-binding norm of responsible State behaviour, and there is currently insufficient State practice and *opinio juris* to support the development of a customary rule containing binding due diligence obligations in cyberspace. Consequently, the article concludes that attempts to establish binding due diligence obligations in cyberspace constitute *lex ferenda* that may be understood as an interventionist attempt by scholars to fill what they perceive to be dangerous legal gaps.

Keywords: public international law, due diligence obligations, cyberspace, cyber operations, information and communication technologies (ICTs).

I. INTRODUCTION

There is currently widespread agreement among States that, in principle, international law applies to State cyber operations. Three consensus reports endorsed by States participating in the United Nations (UN) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), comprising governmental experts from 25 States, have determined that international law, 'in particular the Charter of the United Nations', applies to cyber operations.[1] While the UN GGE reports themselves are non-binding,

[1] UN General Assembly (UNGA), 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of

[*ICLQ* vol 73, January 2024 pp 135–176] doi:10.1017/S0020589323000489

they contain references to both binding and non-binding norms. The 2015 report was subsequently welcomed and endorsed by the UN General Assembly (UNGA) by consensus.[2] The 2021 final report of the UN Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, a parallel process open to all interested States, with participation from the private sector, non-governmental organizations (NGOs) and academia, adopted by consensus among State participants, reaffirmed that international law is applicable to cyber operations.[3] However, while there is broad agreement that international law applies in principle to cyber operations, both fora have encountered disagreements over the inclusion of specific language and references to the application of certain areas of law, for example, the right to self-defence, international humanitarian law and international human rights law.[4]

In the cyber context, due diligence obligations have been discussed in relation to cyber operations which pass through or manifest on infrastructure on the territory of a State and may cause harm in the territory of another State. Despite the clear position of States on the matter in consensus UN GGE reports,[5] the existence and normative scope of binding due diligence obligations in relation to cyber operations is currently the subject of dispute in the literature.[6] Some

International Security' (24 June 2013) UN Doc A/68/98, 8 (2013 GGE Report); UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174, 12 (2015 GGE Report); UNGA, 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' (14 July 2021) UN Doc A/76/135, 17 (2021 GGE Report); Charter of the United Nations (signed 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI. The Group was established pursuant to para 4 of UNGA Res 60/45 (6 January 2006) UN Doc A/RES/60/45.

[2] UNGA Res 70/237 (30 December 2015) UN Doc A/RES/70/237.

[3] UNGA, 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report' (10 March 2021) UN Doc A/AC.290/2021/CRP.2, 2 (OEWG Final Report).

[4] See A Henriksen, 'The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace' (2019) 5 JCybersecurity tyy009; A Väljataga, 'Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly' (*CCDCOE INCYDER*, 1 September 2017) <https://web.archive.org/web/20171109041636/https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html>; F D'Incau and S Soesanto, 'The UN GGE Is Dead: Time to Fall Forward' (*ECFR*, 15 August 2017) <https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance>; E Tikk and M Kerttunen, *The Alleged Demise of the UN GGE: An Autopsy and Eulogy* (Cyber Policy Institute 2017); J Gold, 'Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?' (*Council on Foreign Relations*, 18 March 2021) <https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what>; M Schmitt and L Vihul, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms' (*Just Security*, 30 June 2017) <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/>; J Gold, 'A Cyberspace "FIFA" to Set Rules of the Game? UN States Disagree at Second Meeting' (*Council on Foreign Relations*, 2 March 2020) <https://www.cfr.org/blog/cyberspace-fifa-set-rules-game-un-states-disagree-second-meeting>.

[5] See Section III.A. of this article.

[6] eg, see A Coco and T de Souza Dias, '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law' (2021) 32 EJIL 771, 772–773.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

commentators have sought to encourage the development of due diligence obligations in relation to cyber operations,[7] and others have even sought to assert that binding obligations exist for States as *lex lata*.[8] This article adopts a critical approach towards scholarship asserting that States are under binding due diligence obligations in relation to cyber operations based upon framing due diligence as a universal standalone source from which it is possible to derive binding obligations for all areas of activity. The article demonstrates, by reference to doctrine, the case law of the International Court of Justice (ICJ) and to the existence of areas of activity where only soft-law 'obligations' exist, that due diligence obligations are anchored in specific primary rules and are not a universal standalone source from which it is possible to derive binding obligations for all areas of activity. The article examines the position of States in UN fora that clearly determines that States do not consider themselves to be under such binding obligations, including the UN GGE that explicitly determined by consensus that due diligence in cyberspace constitutes a 'voluntary, non-binding norm of responsible State behaviour',[9] and individual state positions including those that have been influenced by these scholarly debates. The motivations and implications of literature that often encourages the development and/or recognition of binding obligations by States in cyberspace whilst simultaneously claiming that such obligations already exist as a matter of *lex lata* are also addressed. The article concludes that there is currently insufficient State practice and *opinio juris* to support the crystallization or development of a customary rule featuring binding due diligence obligations in cyberspace. Assertions of binding due diligence obligations in cyberspace therefore constitute *lex ferenda.*

The structure of the article is as follows. First, the article examines the status of due diligence obligations in international law to determine that due diligence obligations are anchored in primary rules and are not a universal standalone source from which it is possible to derive binding obligations for all areas of activity. Second, the article discusses the normative relationship between due diligence obligations and cyber operations in light of the position of States and relevant State practice to demonstrate that there is currently insufficient State practice and *opinio juris* to support the development of a customary rule containing binding due diligence obligations in cyberspace. Finally, the article addresses risks and implications associated with construing due diligence as a universal standalone source from which it is possible to derive binding obligations for all areas of activity.

[7] eg, J Kulesza, *Due Diligence in International Law* (Brill Nijhoff 2016) 300–2; MN Schmitt, 'In Defense of Due Diligence in Cyberspace' (2015) 14 YaleLJF 68, 69.

[8] eg, see MN Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017) 30–1; Coco and Dias (n 6).

[9] 2021 GGE Report (n 1) 10.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

II. STATUS OF DUE DILIGENCE OBLIGATIONS

In international law, the term due diligence is invoked in relation to expectations on a State to manage risks emanating from non-State actors on its territory in particular scenarios,[10] though risks may also originate from other causes such as a force of nature or activities of a third-party State.[11] In 2012, the International Law Association (ILA) established a Study Group to examine 'the extent to which there is a commonality of understanding between the distinctive areas of international law in which the concept of due diligence is applied'.[12] The Study Group produced several reports and a resolution that was adopted by an ILA conference in August 2016[13] recognizing 'the importance of due diligence as a relevant standard of conduct in many areas of international law' and the 'continued reliance on due diligence by international courts and tribunals'.[14]

A. Doctrine and Due Diligence Obligations

Questions have risen about the nature of due diligence in terms of the inconsistent characterization of its status in international law.[15] The *Max Planck Encyclopedia of Public International Law* defines due diligence obligations as 'primary obligations that require States … to endeavour to reach the result set out in the obligation' where '[a] breach of these obligations consists not of failing to achieve the desired result but failing to take the necessary, diligent steps towards that end'.[16] Due diligence obligations have been addressed in a number of international courts and arbitral awards[17]

[10] And sometimes beyond the territory of a State, see discussion of ICJ case law below.

[11] A Peters, H Krieger and L Kreuzer, 'Due Diligence in the International Legal Order: Dissecting the Leitmotif of Current Accountability Debates' in H Krieger, A Peters and L Kreuzer (eds), *Due Diligence in the International Legal Order* (OUP 2020) 2.

[12] ILA, 'Study Group on Due Diligence in International Law – Mandate' (International Law Association, 2012) <https://www.ila-hq.org/en_GB/documents/mandate-2>; 'ILA Study Group on Due Diligence in International Law: Second Report' (International Law Association, July 2016) <https://www.ila-hq.org/en_GB/documents/draft-study-group-report-johannesburg-2016>.

[13] 'ILA Study Group on Due Diligence in International Law: First Report' (International Law Association, 7 March 2014) <https://www.ila-hq.org/en_GB/documents/first-report-washington-dc-2014>; ILA, 'Resolution No.8/2016: Study Group on Due Diligence in International Law' (International Law Association, 11 August 2016) <https://www.ila-hq.org/en_GB/documents/conference-study-group-resolution-english-johannesburg-2016>.

[14] ILA, 'Resolution No.8/2016' ibid.

[15] See N McDonald, 'The Role of Due Diligence in International Law' (2019) 68 ICLQ 1041, 1043; Peters, Krieger and Kreuzer (n 11) 8–9.

[16] T Koivurova, 'Due Diligence' in R Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (OUP 2010).

[17] *South China Sea Arbitration* (*Philippines v China*) (Award) PCA Case No 2013-19, ICGJ 495, 744.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

including the ICJ[18] and the International Tribunal on the Law of the Sea (ITLOS).[19]

Due diligence obligations have most commonly developed in treaties concerning international environmental law[20] but they can be found in other branches of international law as well.[21] As Koivurova explains, 'State practice has developed more precise rules and standards as to what due diligence requires of its subjects in certain areas of international relations', where '[m]any fields of international law have seen the emergence of primary obligations that require States to exercise due diligence, that is, to endeavour to reach the result set out in the obligation'.[22]

As demonstrated by its adverbial use, diligence may be understood as a qualifier of behaviour, whereby an actor can behave diligently or negligently.[23] Though the term due diligence has a 'wide array of different meanings and fulfils diverging functions in hugely diverse legal regimes',[24] it is perhaps most coherently invoked in relation to what was traditionally characterized[25] as the no-harm rule and the allocation of accountability for human-made risks in relation to transboundary harm in international environmental law.[26]

The identification of due diligence obligations based in rules of customary international law can be particularly difficult to ascertain and consequently international courts and tribunals have played a significant role in identifying the existence of such obligations in various fields of international law.[27] For

[18] *Corfu Channel Case (UK v Albania)* (Merits) [1949] ICJ Rep 4, 22; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Judgment)* [2007] ICJ Rep 43, para 430; *Pulp Mills on the River Uruguay (Argentina v Uruguay)* (Judgment) [2010] ICJ Rep 14, paras 101, 197, 204, 223; *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v Costa Rica)* (Judgment) [2015] ICJ Rep 665, paras 104, 153, 168, 228.

[19] *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area* (Advisory Opinion of 1 February 2011, Seabed Disputes Chamber) ITLOS Reports 2011, paras 110–112, 117–120, 131–132; *Request for an Advisory Opinion Submitted by the Sub-Regional Fisheries Commission* (Advisory Opinion of 2 April 2015) ITLOS Reports 2015, paras 125–132, 146–150.

[20] Generally, see A Boyle and C Redgwell, *Birnie, Boyle, and Redgwell's International Law and the Environment* (4th edn, OUP 2021) ch 3.

[21] eg, international human rights law, Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence (adopted 11 May 2011, entered into force 1 August 2014) CETS No 210, art 5(1)–(2); also see the development of due diligence obligations in the fields of the law of neutrality and the law of aliens; A Peters, H Krieger and L Kreuzer, 'Due Diligence: The Risky Risk Management Tool in International Law' (2020) 9 CILJ 121, 123; Koivurova (n 16).

[22] Koivurova ibid.

[23] Peters, Krieger and Kreuzer (n 11) 2.

[24] H Krieger and A Peters, 'Due Diligence and Structural Change in the International Legal Order' in Krieger, Peters and Kreuzer (eds) (n 11) 374.

[25] Peters, Krieger and Kreuzer (n 21) 127–9.

[26] Krieger and Peters (n 24) 374.

[27] Peters, Krieger and Kreuzer (n 11) 11.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

instance, as established by international courts and tribunals,[28] and affirmed by other sources such as the 1992 Rio Declaration[29] and the International Law Commission's (ILC's) 2001 Draft Articles on Prevention of Transboundary harm,[30] two rules of customary international law have developed in international environmental law.[31] First, that States have a duty to take appropriate measures to prevent, reduce and control transboundary pollution and environmental harm that results from activities within their jurisdiction or control. Second, States have a duty to cooperate in mitigating transboundary risks and emergencies through processes of notification, consultation, negotiation, and, where appropriate, environmental impact assessments. However, neither rule constitutes a complete prohibition on all transboundary harm,[32] and 'it is erroneous (and deeply confusing) to refer to a "no harm" rule in this context', as '[t]he obligation is one of conduct, not of result'.[33] Due diligence obligations do not require that harm to the interests of other States is totally prevented, only that States make best efforts to prevent or minimize such harm.[34] Due diligence obligations may be procedural in notifying or reporting certain events and in warning other States, or institutional in States being obliged to take legislative or administrative safeguard measures.[35]

The work of the ILA encouraged further research on due diligence obligations and their status in international law, perhaps most substantially, a project at the Max Planck Institute for Comparative Public Law and International Law that sought to determine 'whether a common understanding of due diligence throughout the different areas of international law and possibly across different types of legal persons (States, IOs [international organizations], other) can be traced and, if so, whether this warrants qualifying due diligence as an overarching principle of international law',[36] resulting in several comprehensive publications on the subject.[37]

[28] See *Pulp Mills* (n 18) paras 101, 197, 204, 223; and *Request for an Advisory Opinion Submitted by the Sub-Regional Fisheries Commission* (n 19) paras 110–112, 117–120, 131–132.

[29] UNGA, 'Report of the United Nations Conference on Environment and Development (Rio de Janeiro, 3–14 June 1992)' (12 August 1992) UN Doc A/CONF.151/26 (Vol. I).

[30] ILC, 'Report of the International Law Commission on the Work of its Fifty-Third Session' (23 April–1 June, 2 July–10 August 2001) UN Doc GAOR A/56/10, Text of the Draft Articles with Commentaries Thereto: Prevention of Transboundary Harm from Hazardous Activities, 144–170.

[31] Boyle and Redgwell (n 20) 152–3.

[32] 'The duty of due diligence … is not intended to guarantee that significant harm be totally prevented, if it is not possible to do so', ILC (n 30) commentary to art 3, 154.

[33] Boyle and Redgwell (n 20) 153; ILC, 'Report of the International Law Commission on the Work of its Forty-Sixth Session (2 May–22 July 1994) UN Doc A/49/10, Draft Articles on the Law of the Non-Navigational Uses of International Watercourses, commentary to art 7, 103.

[34] ILC (n 30) commentary to art 3, 154.

[35] Peters, Krieger and Kreuzer (n 21) 124–5; Peters, Krieger and Kreuzer (n 11) 12.

[36] Max Planck Institute for Comparative Public Law and International Law, 'Due Diligence in International Law: About the Project' <https://web.archive.org/web/20210508170443/https://www.mpil.de/en/pub/research/areas/public-international-law/due-diligence-in-international.cfm>.

[37] Krieger, Peters and Kreuzer (eds) (n 11); Peters, Krieger and Kreuzer (n 21).

The ambitious argument has been made that there exists a coherent general principle of due diligence that spans across all areas of international law.[38] Peters, Krieger and Kreuzer address the significance of a distinction between due diligence understood as a general principle, obligation or duty, or standard:

> As a general principle, due diligence would also have to be read and construed in the light of other international legal principles, such as sovereignty or good neighbourliness. Understood as an 'obligation' or 'duty', the function and content of due diligence would likely remain more constrained by the specific norm to which it attaches. A 'standard' of due diligence would rather neutrally suggest a normative expectation.[39]

However, the treatment of due diligence by international courts and tribunals clearly determines that there is no broad or 'standalone' rule of customary international law, nor general principle in the sense of Article 38(1)(c) of the ICJ Statute, requiring States to exercise due diligence that spans across all areas of international law.[40]

B. Case Law and Due Diligence Obligations

Rather than recognizing due diligence as a 'free-standing' concept in international law, the ICJ recognizes binding obligations upon a State to act with due diligence as part of an existing primary rule, or where the Court otherwise seeks to determine the content of treaty or customary law rules that may or may not explicitly refer to 'due diligence'.[41] In other words, after first identifying the relevant rules of international law applicable to the situation in question, the Court then seeks to determine what standard of review the rule may require a State to undertake, either explicitly or implicitly, to act consistently with the rule. The Court's approach to due diligence obligations underlines that they require a primary rule in order for such obligations to arise and that the nature of a legal obligation to act with due diligence is specific to a particular context and so should not be universally transposable across one area of international law to another.[42]

The term due diligence was used as far back as 1871 in a treaty between the United States (US) and United Kingdom (UK) that led to the *Alabama Claims* arbitration.[43] The resulting Alabama Arbitration Award of 1872, occasionally still cited in relation to the contemporary status of due diligence obligations in international law, concerned primary rules in the form of a treaty in relation to

[38] eg, see Kulesza (n 7).
[39] Peters, Krieger and Kreuzer (n 11) 9.
[40] See McDonald (n 15) 1045–8; and Peters, Krieger and Kreuzer (n 21).
[41] McDonald ibid 1044; A Ollino, *Due Diligence Obligations in International Law* (CUP 2022) 57.
[42] McDonald ibid 1044–5.
[43] Art 6 of the Washington Treaty (1871) between the US and the UK, entered into as a means to conclude the *Alabama Claims*.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

activities at sea,[44] though the arbitrators' ruling on what constituted due diligence was never accepted internationally among States.[45] The term is also associated with the *Trail Smelter* arbitration,[46] an ad hoc arbitration implemented by the US and Canada in a 1935 bilateral treaty to settle a dispute concerning air pollution emanating from Canada into the US, the resulting awards of which are considered the '*locus classicus* and *fons et origio*' within the area of international environmental law.[47]

In 1949 in its first contentious case, *Corfu Channel*, the ICJ addressed obligations of due diligence, but only did so in relation to a corresponding primary rule of international law.[48] The case concerned an incident in 1946 in which British warships passing through Albanian territorial waters were severely damaged by naval mines, resulting in the loss of life of 44 sailors. The issue before the Court was not whether Albania had exercised due diligence, but rather which response was required having established actual knowledge of the mines under customary international law.[49] The Court elaborated in general terms on the nature of Albania's legal obligations in relation to the minefield within their territorial waters as follows:

> The obligations incumbent upon the Albanian authorities consisted in notifying, for the benefit of shipping in general, the existence of a minefield in Albanian territorial waters and in warning the approaching British warships of the imminent danger to which the minefield exposed them. Such obligations are based … on certain general and well-recognized principles, namely: elementary considerations of humanity, even more exacting in peace than in war; the principle of the freedom of maritime communication; and every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.[50]

The judgment of the Court clearly underlines that although Albania was under an obligation to act with due diligence in relation to the minefield, that legal obligation emanated from primary rules of international law in relation to that discrete context, specifically, the right of innocent passage and the concomitant

[44] *Alabama Claims of the United States of America against Great Britain*, Award rendered on 14 September 1872 by the tribunal of arbitration established by art I of the Treaty of Washington of 8 May 1871.

[45] R Brent, 'The Alabama Claims Tribunal: The British Perspective' (2022) 44 IntlHistRev 21, 58.

[46] *Trail Smelter Arbitration* (*United States v Canada*), Ad Hoc International Arbitral Tribunal (11 March 1941) 3 UNRIAA 1911, 1938.

[47] RA Miller, 'Trail Smelter Arbitration' in R Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (OUP 2007). The *Trail Smelter* Awards have found tracking within the ICJ in the context of international environmental law, eg, in the *Gabčíkovo-Nagymaros Case* the Court stated that '[t]he existence of the general obligation of States to ensure that activities within their jurisdiction and control respect the environment of other States or of areas beyond national control is now part of the corpus of international law relating to the environment', *Case concerning the Gabčíkovo-Nagymaros Project* (*Hungary v Slovakia*) (Judgment) [1997] ICJ Rep 7, para 53.

[48] *Corfu Channel* (n 18) 22.

[49] M Waibel, 'Corfu Channel Case' in R Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (OUP 2013).

[50] *Corfu Channel* (n 18) 22.

obligation of the coastal States not to hamper this right.[51] As explained by Heathcote:

> … when it comes to responsibility for wrongful acts, it is only in relation to established rights that an obligation of due diligence is owed by one State to another (in the *Corfu Channel* case, the right of innocent passage).[52]

The *Pulp Mills* case concerned whether or not Uruguay had breached its primary obligations under the Statute of River Uruguay, a 1975 bilateral treaty that sought to govern the use by each State of those parts of the River Uruguay which formed a common border between them.[53] In interpreting the nature and extent of Uruguay's obligations under the bilateral treaty, the Court looked to other primary rules of customary international law in accordance with the Vienna Convention on the Law of Treaties.[54] The Court stated that 'the principle of prevention, as a customary rule, has its origins in the due diligence that is required of a State in its territory',[55] that '[t]his Court has established that this obligation "is now part of the corpus of international law relating to the environment"', where this rule required a State to use 'all the means at its disposal' 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'.[56] *Pulp Mills* demonstrates that the ICJ identifies obligations of due diligence for States only to the extent that they exist within a specific primary treaty rule or rule of customary international law within the particular context of the scenario in question, in this instance, the field of international environmental law.

In *Armed Activities*,[57] the Court considered allegations filed by the Democratic Republic of Congo (DRC) that Uganda had 'breached its obligation of vigilance incumbent upon it as an occupying Power by failing to enforce respect for human rights and international humanitarian law' on its territory.[58] This 'obligation of vigilance' is, however, anchored in specific treaty provisions that were invoked by the DRC that claimed violations thereof

[51] The basis of the UK claim is that the ships in question were exercising their right of innocent passage, *Corfu Channel* (n 18) 10; the Court refers to the right of innocent passage throughout the judgment, eg, recognizing that '[i]t is, in the opinion of the Court, generally recognized and in accordance with international custom that States in time of peace have a right to send their warships through straits used for international navigation between two parts of the high seas without the previous authorization of a coastal State, provided that the passage is *innocent*. Unless otherwise prescribed in an international convention, there is no right for a coastal State to prohibit such passage through straits in time of peace.' ibid 28 (emphasis in original).

[52] S Heathcote, 'State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility' in K Bannelier, T Christakis and S Heathcote (eds), *The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case* (Routledge 2012) 299.

[53] *Pulp Mills* (n 18).

[54] Vienna Convention on the Law of Treaties (signed 23 May 1969, entered into force 27 January 1980) 1155 UNTS 331.

[55] *Pulp Mills* (n 18) para 101.

[56] ibid.

[57] *Armed Activities on the Territory of the Congo (Democratic Republic of Congo v Uganda)* (Judgment) [2005] ICJ Rep 168.

[58] ibid, para 189.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

through Uganda's occupation of its territory.[59] The findings of the Court that Uganda violated international law obligations 'by its failure, as an occupying Power, to take measures to respect and ensure respect for human rights and international humanitarian law in Ituri district'[60] was based on the breach of such treaty provisions in relation to the exercise of control over the territory in question, and consequently the obligation to act with due diligence as per the treaty provisions.

Finally, the Court's approach in the *Prevention and Punishment of the Crime of Genocide* case provides a yet clearer explanation of the nature of due diligence obligations in international law.[61] The case concerned alleged violations of the Convention on the Prevention and Punishment of the Crime of Genocide, as well as various matters which Bosnia and Herzegovina claimed were connected therewith, including the allegation that under Article I Serbia failed in its duty to prevent genocide by not acting to prevent the Srebrenica massacre in 1995. The Court's treatment of due diligence clearly understands such obligations as being contained within primary rules in relation to the specific context of the situation in question. Indeed, the Court explicitly cautions against the transposition of due diligence obligations from one area of international law to another,[62] recognizing that similar 'obligations to prevent' existed in various treaties[63] but that the content of the obligations to act with due diligence was not comparable between treaty regimes and different rules of customary international law.[64] In other words, the Court recognized that due diligence obligations are based in primary rules, warned against a generalization of due diligence obligations between different rules, and stated that the context and regime in which such obligations were developed by States are paramount:[65]

> The content of the duty to prevent varies from one instrument to another, according to the wording of the relevant provisions, and depending on the nature of the acts to be prevented … … The decision of the Court *does not, in this case, purport to establish a general jurisprudence applicable to all cases*

[59] The DRC alleged breaches of arts 27, 32 and 53 of the fourth Geneva Convention.

[60] ibid, para 345.

[61] *Prevention and Punishment of the Crime of Genocide* (n 18).

[62] ibid, para 429.

[63] The Court cited Convention against Torture and Other Cruel, Inhuman and Degrading Treatment or Punishment (adopted 10 December 1984, entered into force 26 June 1987) 1465 UNTS 85, art 2; Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, Including Diplomatic Agents 1973 (adopted 14 December 1973, entered into force 20 February 1977) 1035 UNTS 167, art 4; Convention on the Safety of United Nations and Associated Personnel 1994 (adopted 9 December 1994, entered into force 15 January 1999) 2051 UNTS 363, art 11; and International Convention on the Suppression of Terrorist Bombings (adopted 15 December 1997, entered into force 23 May 2001) 2149 UNTS 256, art 15.

[64] McDonald (n 15) 1047–8. As Peters et al observe: 'anyone who wants to identify and circumscribe, in a more exacting way, the due diligence obligations (both procedural and substantive) must always look at the substantive standards of the specific regime. This is what the ICJ opined in the *Bosnian Genocide* case, with regard to the related obligation of prevention.' Peters, Krieger and Kreuzer (n 21) 133.

[65] Peters, Krieger and Kreuzer ibid 133.

> *where a treaty instrument, or other binding legal norm, includes an obligation for States to prevent certain acts*.[66]

In *Border Area/Road*, the Court was called upon to apply procedural and substantive rules of customary international law and treaty provisions, where in each case the Court examined the relevant primary rule(s) to determine whether obligations were applicable.[67] However, the Court concluded that Nicaragua had not proved that the construction of the road caused significant transboundary harm, and accordingly dismissed Nicaragua's claims on this point.[68]

Critically, these cases also illustrate that States do not refer to a universal standalone source of due diligence obligations in international law in their pleadings before the ICJ; instead they invoke specific primary rules in the form of treaty law or custom that require a particular act or omission by other States that may include requiring a State to act with due diligence.[69] As Ollino notes, '[f]rom the perspective of due diligence … it does not appear that the court used due diligence per se as a free-standing source of obligations for states'.[70] The approach of the ICJ is first to identify relevant primary rules before considering any due diligence obligations required by those rules in the context of the particular scenario in question, where the nature of such obligations by reference to a specific rule will differ from case to case.[71] This approach is consistent with the findings of tribunals in other areas of law, for example, in the law of the sea it is clear that '[due diligence obligations apply] in all those cases in which a treaty provision or rule of customary international law requires a State "to ensure" a certain result or to reach a certain aim, be it the avoidance of a certain harm or the achievement of a certain result'.[72]

As Crawford notes in his commentary to the ILC Articles on State Responsibility:

> … *different primary rules of international law* impose different standards ranging from 'due diligence' to strict liability, and that breach of the correlative obligations gives rise to responsibility without any additional requirements. *There does not appear to be any general principle or presumption about the role of fault in*

[66] *Prevention and Punishment of the Crime of Genocide* (n 18) para 429 (emphasis added).
[67] *Certain Activities Carried out by Nicaragua and Construction of a Road in Costa Rica* (n 18).
[68] ibid, para 105.
[69] As stated by McDonald, 'it is not to an "obligation of due diligence" as such which the ICJ looks in any given case, but to the applicable rules of international law. The exercise carried out by the Court is one of examining: a] the scope of the customary rule, or extent of jurisdiction of the treaty regime which is alleged to have been breached; b) the level of control exerted, or of jurisdiction exercised, by the State in order to determine any corresponding obligation; and c] whether the State's responsibility is engaged through its actions. Due diligence may feature as an idea within any of these analyses by reference to a primary rule.' McDonald (n 15) 1048–9.
[70] Ollino (n 41) 54.
[71] McDonald (n 15) 1048.
[72] I Papanicolopulu, 'Due Diligence in the Law of the Sea' in Krieger, Peters and Kreuzer (eds) (n 11) 150.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

relation to any given primary rules, since it depends on the interpretation of that rule in the light of its object or purpose. Nor should there be, since the functions of different areas of the law, all underpinned by State responsibility, vary so widely.[73]

C. Conclusion

Due diligence is therefore not a free-standing obligation but a 'modality attached to a duty of care for someone or something else (including the duty to prevent and mitigate harm)'; indeed, '[o]ne might call it an ancillary obligation if one wants to use the language of obligation at all'.[74] As McDonald explains, 'there is no "general principle of due diligence" in international law', 'a legal requirement to exercise due diligence may be a component part of a primary rule of international law, but this can only be determined by referring back to the primary rule in question'.[75] It is precisely in this manner that this article employs the term 'obligations' in relation to due diligence, that is, an ancillary obligation of conduct that forms a component part of a primary rule of international law.[76] Regardless over the confusion surrounding the status and use of various terminology invoked in referring to the status of due diligence obligations in international law, it is generally accepted that binding obligations are anchored in primary rules and that due diligence obligations are not an independent free-standing source of such obligations. For instance, Ollino considers that 'due diligence is not a free-standing obligation that is, per se, a source of rights and duties for states. It is a notion that is necessarily "attached" to primary rules, whether customary or conventional, and that depends on these rules to be clearly defined'.[77] Similarly, for Peters, Krieger and Kreuzer, '[a]s a norm or standard, due diligence is a requirement to behave diligently. And this standard of due diligence is, in law, necessarily *ancillary* to some (other) legal obligation and no free-floating obligation itself';[78] 'due diligence cannot be characterised as a general principle of international law due to its diverse content in different fields of international law and its dependence on accompanying primary rules … [i]t is therefore immaterial whether due diligence is indeed sufficiently widespread in representative legal orders to qualify as a general principle in the sense of art 38(1)(c) of the ICJ Statute'.[79]

The role and function of due diligence obligations differ from one area of international law to another where their inclusion in primary rules has been developed by States to apply to the specific attributes of each area.[80] International human rights law involves positive obligations to protect

[73] J Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* (CUP 2005) 13 (emphasis added).
[74] Peters, Krieger and Kreuzer (n 11) 2.
[75] McDonald (n 15) 1041.
[76] See *Responsibilities and Obligations of States* (n 19) para 110; *Pulp Mills* (n 18) para 187.
[77] Ollino (n 41) 57.
[78] Peters, Krieger and Kreuzer (n 21) 122 (emphasis in original).
[79] ibid 121, 134 (fn 58).
[80] ibid 132.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

individuals, whereas international economic law involves 'due diligence' processes that are significantly divergent from 'due diligence' as a standard of behaviour in the context of the traditional no-harm rule that may involve conducting a legal, environmental and/or social audit prior to undertaking projects or other (legal) undertakings.[81] Indeed, even within particular areas of international law one must be careful drawing general conclusions about obligations from the limited context of certain precedents.[82] As McDonald concludes:

> … due diligence within international law is something which requires a primary rule to be relevant. The ICJ also supports the idea that the nature of a legal obligation to act with due diligence in a given instance relies upon context, and due diligence obligations should thus not be read across from one area of international law to another.[83]

Crawford supports this understanding, citing the ICJ in *Pulp Mills*, stating that:

> [w]hile it is doubtful whether courts will be willing to impose responsibility for transboundary damage on States in the absence of an express obligation, specific regimes have been advanced for establishing different means of legal redress in the case of environmental harm.[84]

Finally, in consideration of State practice it is important to note that States undertake what may be construed as activities related to performing due diligence, for example, by introducing policy guidance for their officials, some elements of which may be a consequence of a legal requirement and some of which may not, for instance where States perform such activities for policy reasons.[85] Such activities may be irrelevant as State practice in any attempt to identify a primary rule of customary international law encompassing due diligence obligations if the practice is not undertaken with the required conviction that a legal right or obligation is involved, that is, acceptance as law, or *opinio juris*.[86]

III. DUE DILIGENCE OBLIGATIONS AND CYBER OPERATIONS

A. The Position of States in UN Fora

Following decades of debate on the application of international law to cyber operations, in the 2021 UN GGE Report adopted by consensus, States,

[81] ibid 132–3. [82] See Boyle and Redgwell (n 20) 218. [83] McDonald (n 15) 1045.
[84] J Crawford, *Brownlie's Principles of Public International Law* (9th edn, OUP 2019) 544.
[85] See McDonald (n 15) 1049–54.
[86] As reflected by the ILC's Draft Conclusions on Identification of Customary International Law, '[t]o determine the existence and content of a rule of particular customary international law, it is necessary to ascertain whether there is a general practice among the States concerned that is accepted by them as law (*opinio juris*) among themselves', ILC, 'Report of the International Law Commission, Seventieth Session' (30 April–1 June and 2 July–10 August 2018) UN Doc A/73/10, Draft Conclusions on Identification of Customary International Law, 154.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

including the five permanent members of the UN Security Council,[87] explicitly determined due diligence in cyberspace constitutes a 'voluntary, non-binding norm of responsible State behaviour' using non-mandatory language, including that 'States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs':

> This norm reflects an expectation that if a State is aware of or is notified in good faith that an internationally wrongful act conducted using ICTs is emanating from or transiting through its territory it will take all appropriate and reasonably available and feasible steps to detect, investigate and address the situation. It conveys an understanding that a State should not permit another State or non-State actor to use ICTs within its territory to commit internationally wrongful acts.[88]

This language is used in the explicit and deliberate context of a clear section on non-binding norms of responsible State behaviour, which is separate and distinct from the section of the report on binding international law and rules of international law. As the 2021 Report explains on the relationship and distinction between international law and voluntary, non-binding norms of responsible State behaviour:

> The Group reaffirms with regard to the use of ICTs by States that voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. Norms and existing international law sit alongside each other. *Norms do not seek to limit or prohibit action that is otherwise consistent with international law. They reflect the expectations of the international community and set standards for responsible State behaviour* …
>
> Given the unique attributes of ICTs, the Group reaffirms the observation of the 2015 report that additional norms could be developed over time, and, separately, notes the possibility of future elaboration of additional binding obligations, if appropriate.[89]

The previous consensus 2015 UN GGE Report also addressed due diligence as the basis for a voluntary, non-binding norm of responsible State behaviour[90] following State representatives in the UN GGE process reportedly resisting the development of binding due diligence obligations in cyberspace.[91] The 2015 report was subsequently welcomed and endorsed by the UNGA by consensus.[92]

[87] Including Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, Netherlands, Norway, Romania, Russian Federation, Singapore, South Africa, Switzerland, UK, US and Uruguay; see 2021 GGE Report (n 1). [88] 2021 GGE Report (n 1) 10. [89] ibid 8 (emphasis added).

[90] 2015 GGE Report (n 1) 7, 8.

[91] DB Hollis, 'International Law and State Cyber Operations: Improving Transparency' (21 January 2019) OEA/Ser.Q, CJI/doc. 578/19, 2 <http://www.oas.org/en/sla/iajc/docs/CJI_doc_578-19.pdf>; AM Sukumar, 'The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?' (*Lawfare*, 4 July 2017) <https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>.

[92] UNGA Res 70/237 (n 2).

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

The 2021 consensus UN OEWG Final Report that was open to involvement from all States and which also featured extensive discussion of due diligence obligations was unable to agree on the inclusion of any such language, even in vague non-binding terms, with the reference to due diligence obligations that initially appeared in the zero draft of the report relegated to the Chair's Summary outlining issues deemed too controversial for the main text.[93] This further demonstrates that States do not consider binding due diligence obligations exist or have been developed in relation to cyber operations.

The precise language of consensus reports of the UN GGE and UN OEWG was fiercely contested by States and involved extensive discussion of applicable international law.[94]

B. Attempts to Identify Binding Obligations

The idea that there might exist a primary standalone universal due diligence 'rule' of customary international law is at odds with the treatment of such obligations by the ICJ and established literature outside the context of cyber operations.[95] Several commentators have characterized due diligence as a broad general principle of international law and sought to make arguments highlighting the benefits of why States should recognize, or effectively develop, binding due diligence obligations for cyber operations.[96] Despite the clear position of States in UN fora to the contrary, several academic projects and commentators have even sought to argue that States are under binding due diligence obligations in relation to cyber operations that emanate on or transit through their territory as a matter of *lex lata*.[97] These authors have adopted various unconvincing and ultimately flawed approaches as a basis for such arguments that ultimately rely on construing due diligence as a universal standalone source from which it is possible to identify binding obligations applicable to all areas of activity based primarily on a misrepresentation of the *Corfu Channel* judgment. Recently, a project at the University of Oxford's Institute for Ethics, Law and Armed Conflict led by Akande, Dias

[93] See references made, in particular, in UNGA, 'Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Chair's Summary' (10 March 2021) UN Doc A/AC.290/2021/CRP.3, Annex, 10–20.

[94] See Henriksen (n 4); Väljataga (n 4); D'Incau and Soesanto (n 4); Tikk and Kerttunen (n 4); Gold, 'Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?' (n 4); Schmitt and Vihul (n 4); Gold, 'A Cyberspace "FIFA" to Set Rules of the Game?' (n 4).

[95] See analysis in Section II of this article.

[96] See Kulesza (n 7) 300–2; Schmitt (n 7); for an exploration of relevant ICJ jurisprudence on this subject, see T Mikanagi, 'Application of the Due Diligence Principle to Cyber Operations' (2021) 97 IntlLStud 1019.

[97] Schmitt (n 8) 30; R Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016) 21 JC&SL 429; F Delerue, *Cyber Operations and International Law* (CUP 2020) 353–75, 358.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

and Coco, funded by the Japanese Government,[98] made allegedly distinct, but upon inspection ostensibly similar assertions, claiming States are under 'a patchwork' of protective binding due diligence obligations in relation to cyber operations on their territory.[99] In the light of clear evidence contradicting the status of due diligence as a universal standalone source that is directly transposable to different areas or regimes to identify binding obligations,[100] the main issue faced by those arguing that States are under due diligence obligations in relation to cyber operations is surmounting the issue of locating such obligations in a primary rule or rules.

1. Encouragement for the development of due diligence obligations

Kulesza, who made a comprehensive argument in a 2016 monograph that due diligence is a general principle of international law,[101] then suggested that we were heading 'toward a due diligence standard for cyberspace'.[102] The argument by Kulesza appears to maintain that due diligence is a principle that is universally relevant to all areas of activity while at the same time claims that States are heading towards developing the content and scope of binding obligations in the context of cyber operations. Such an argument demonstrates exactly why States have developed primary rules containing

[98] Japan is a State that is keen to establish obligations of due diligence in cyberspace. Japan asserts that 'States have a due diligence obligation regarding cyber operations under international law', whilst also noting that '[t]he outer limit of the due diligence obligation of territorial States with respect to cyber operations is not necessarily clear', UNGA, 'Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266' (13 July 2021) UN Doc A/76/136, 48; Ministry of Foreign Affairs of Japan, 'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations' (28 May 2021) 5–6 <https://www.mofa.go.jp/files/100200935.pdf>; Oxford Institute For Ethics, Law and Armed Conflict, 'Cyber Due Diligence' <https://www.elac.ox.ac.uk/research/cyber-due-diligence/>.

[99] A Coco and T de Souza Dias, 'Part I: Due Diligence and COVID-19: States' Duties to Prevent and Halt the Coronavirus Outbreak' (*EJIL: Talk!*, 24 March 2020) <https://www.ejiltalk.org/part-i-due-diligence-and-covid-19-states-duties-to-prevent-and-halt-the-coronavirus-outbreak/>; T de Souza Dias and A Coco, 'Part II: Due Diligence and COVID-19: States' Duties to Prevent and Halt the Coronavirus Outbreak' (*EJIL: Talk!*, 25 March 2020) <https://www.ejiltalk.org/part-ii-due-diligence-and-covid-19-states-duties-to-prevent-and-halt-the-coronavirus-outbreak/>; T de Souza Dias and A Coco, 'Part III: Due Diligence and COVID-19: States' Duties to Prevent and Halt the Coronavirus Outbreak' (*EJIL: Talk!*, 25 March 2020) <https://www.ejiltalk.org/part-iii-due-diligence-and-covid-19-states-duties-to-prevent-and-halt-the-coronavirus-outbreak/>; T Dias and A Coco, *Cyber Due Diligence in International Law* (Oxford Institute for Ethics, Law and Armed Conflict 2022) <https://www.elac.ox.ac.uk/wp-content/uploads/2022/02/Final-Report-BSG-ELAC-CyberDueDiligenceInInternationalLaw.pdf>; Coco and Dias (n 6).

[100] See discussion of ICJ case law above, in particular the *Genocide* case, where the Court recognized that due diligence obligations are based in primary rules and explicitly cautioned against the transposition of the content of due diligence obligations from one area of international law to another, *Prevention and Punishment of the Crime of Genocide* (n 18) para 429.

[101] Kulesza (n 7).

[102] ibid 300–2.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

due diligence obligations in relation to specific areas with unique attributes: the unique attributes in those discrete contexts inform the development of the content and scope of obligations in primary rules, as Kulesza explores in great detail in various areas where such obligations have been developed.[103] Indeed, Kulesza extensively details the difficult but necessary process required to develop the content of such obligations for cyber operations,[104] and the language of the argument clearly indicates that such binding obligations have not yet been recognized or developed by States. Kulesza goes on to argue that '[d]ue diligence in cyberspace offers a noteworthy alternative to the still arguable and strongly disputed military qualification of cyberattacks, attempting to view them as acts of armed aggression, possibly allowing an armed response'.[105] In this sense, the attempt to construe due diligence as a general principle in this manner has been adopted to provide a broader basis from which to recognize or develop primary rules containing binding due diligence obligations in areas where they have not yet been established.

In a 2015 article, Schmitt, the director of the *Tallinn Manual* projects, openly acknowledged extensive 'opposition [from States] to due diligence in international cyber law' and discussed the 'consequences of opposing the due diligence obligation', with States being 'conflicted' over whether to commit to recognizing or developing specific due diligence obligations in the context of cyber, which he observed would serve to hamper their own operations as well as that of other actors, or to avoid such regulation and maintain operational freedom but allow others to do the same.[106] Schmitt argued that the benefits for States of recognizing binding due diligence obligations for cyber operations outweigh the risks of not doing so, in what is clearly a *lex ferenda* proposal demonstrating frustration over States having failed to do so:

> On the one hand, if states build 'normative firewalls' by adopting interpretations of the existing law that restrict cyber operations, they will paradoxically also limit their own freedom of action in cyberspace. Alternatively, any interpretive crystallization that safeguards the margin of discretion enjoyed by state's vis-à-vis cyber activities necessarily leaves their cyber systems at risk. Since states accordingly find themselves conflicted when trying to make legal-policy decisions regarding cyber norms, virtually all in-depth work in the field has emerged from the academy. This is an unfortunate reality with deleterious consequences for international law making.[107]

Notably, this publication by Schmitt that encourages States to recognize or develop binding due diligence obligations in relation to cyber operations and which identifies significant opposition from States to do so was published in 2015, only a year before the findings of the *Tallinn Manual 2.0* were adopted

[103] Including due diligence obligations in international environmental law, law of the sea, law of international watercourses, protection of foreigners, and law of diplomatic relations, see ibid 221–61.
[104] ibid 301. [105] ibid 300. [106] Schmitt (n 7) 71–9. [107] ibid 69.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

in 2016 (published in 2017), which confidently asserts such binding obligations exist as *lex lata*, despite no significant progress or change in the positions of States. Furthermore, the original *Tallinn Manual* published in 2013 recognized significant disagreements among the Group of Experts relating to the application of due diligence obligations in the cyber context.[108]

In each of these texts that were published prior to the *Tallinn Manual 2.0*, the mere fact that the authors encourage States to recognize or develop due diligence obligations for cyber operations is a testament that such obligations do not exist.

2. *Assertions of obligations as* lex lata

Specifically, the *Tallinn Manual 2.0* contends that based upon the assertion that due diligence is a general principle of international law, '[a] [S]tate must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States'.[109] While the underlying argument that due diligence should be recognized as a general principle of international law has been made in several ambitious academic publications,[110] such a position is clearly at odds with the status of due diligence obligations in international law, as recognized by international courts and tribunals discussed in the previous section of this article. It is certainly by no means an uncontroversial position, nor commonly accepted, and to present it as such is misleading and clearly has been carefully adopted to construct a foundation to assert that States are under binding due diligence obligations in relation to cyber operations on their territory.

The *Manual* refers to a 'due diligence principle', which it claims 'is the term most commonly used with respect to the obligation of States to control activities on their territory', though no specific citations are provided of the term used in this manner.[111] According to its text, '[due diligence] is a general principle that has been particularised in specialised regimes of international law',[112] presumably in the sense of Article 38(1)(c) of the ICJ Statute. The assertion that due diligence is a general principle of international law and that 'States must exercise due diligence in ensuring territory and objects over which they enjoy sovereignty are not used to harm other States' appears to be based primarily on a misrepresentation of the ICJ's *Corfu Channel* judgment. As the *Manual* states:

> A dictum in the International Court of Justice's *Corfu Channel* judgment, which observes that 'it is every State's obligation not to allow knowingly its territory to

[108] MN Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013) 26–9. [109] Schmitt (n 8) 30. [110] See Kulesza (n 7). [111] Schmitt (n 8) 30. [112] ibid 31.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

> be used for acts contrary to the rights of other States', sets forth the generally recognised contemporary definition of the due diligence principle.[113]

Consequently, the *Manual* claims that '[p]roperly understood, due diligence is the standard of conduct expected of States when complying with this principle', and that '[i]t is a principle that is reflected in the rules, and interpretation thereof, of numerous specialised regimes of international law'.[114] However, the very existence of a category of 'general principles of law formed within the international legal system' remains highly controversial in the ongoing work of the ILC on the topic of *General principles of law*, where significant concerns have been raised within the Commission and the Sixth Committee that the recognition of such a category risks undermining customary international law as a method of identifying primary rules by effectively serving as a 'custom-lite'[115] without the requirement of *opinio juris.*[116] It is precisely this flexibility that the editors appear to seek to exploit in making such a claim, circumventing the lack of State practice and *opinio juris* for a rule of custom containing binding due diligence obligations in cyberspace.[117]

As explained in the previous section of this article, in *Corfu Channel* the Court clearly identified that the legal obligation emanated from primary rules of international law in relation to that discrete context, specifically, the obligation to respect and not to hamper the right of innocent passage.[118] More importantly, this has since been reaffirmed in other cases where the Court has dealt with due diligence obligations, which as explained have confirmed that the approach of the Court is first to identify relevant primary rules before considering any due diligence obligations required by those rules in the context of the particular scenario in question. The *Manual* is correct that primary rules containing due diligence obligations exist in 'specialised regimes' where States have endeavoured to develop them in the context of those

[113] ibid, citing *Corfu Channel* (n 18) 22.

[114] Schmitt ibid 30; and that '[t]he Experts further observed that the due diligence principle has long been reflected in jurisprudence; it is a general principle that has been particularised in specialised regimes of international law', ibid 31.

[115] J Klabbers, *International Law* (2nd edn, CUP 2017) 38.

[116] See M Wood, 'Customary International Law and the General Principles of Law Recognized by Civilized Nations' (2019) 21 ICLR 307; M Vázquez-Bermúdez and A Crosato, 'General Principles of Law: The First Debate within the International Law Commission and the Sixth Committee' (2020) 19 ChineseJIL 157, 168–71; O Pomson, 'General Principles of Law Formed Within the International Legal System?' (*EJIL: Talk!*, 12 July 2022) <https://www.ejiltalk.org/general-principles-of-law-formed-within-the-international-legal-system/>.

[117] The *Tallinn Manual 2.0* states that 'because State cyber practice is mostly classified and publicly available expressions of *opinio juris* are sparse, it is difficult to definitively identify any cyber-specific customary international law', Schmitt (n 8) 3; Wood, the Special Rapporteur of the ILC's work on the identification of customary international law, considers that the requirements for the identification and development or evolution of customary international law share the same twin criteria of State practice and *opinio juris*, M Wood, 'The Evolution and Identification of the Customary International Law of Armed Conflict' (2018) 51 VandJTransnatlL 727, 728, citing ILC, ' Report of the International Law Commission: Sixty-eighth Session' (2 May–10 June and 4 July–12 August 2016) UN Doc A/71/10, 81.

[118] *Corfu Channel* (n 18) 10.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

scenarios, but the key point is that, as confirmed by the approach of the Court, such obligations must be anchored in primary rules. The fact that those seeking to represent due diligence as a universal standalone source do so by taking advantage of the relatively open phrasing of the *Corfu Channel* judgment alone is revealing in their circumvention of the clearer subsequent judgments of the Court on the nature of due diligence obligations. The *Manual*'s assertion that '[due diligence] is a principle that is reflected in the rules, and interpretation thereof, of numerous specialised regimes of international law'[119] does nothing to establish what primary rule such obligations are contained within in relation to cyber operations. Even the nature of due diligence obligations under any specific rule may vary from case to case.[120] For instance, in relation to due diligence obligations, the control of territory alone is not necessarily sufficient to establish the responsibility of a State for actions occurring therein.[121]

Unlike traditional kinetic operations, cyber operations depend on the internet which is almost exclusively transmitted by terrestrial and undersea fibre-optic cables that pass through the territory of multiple States without regard for borders. Even mundane operations such as sending an email from one recipient to another will often pass through the territory of numerous States to be stored on servers on the territory of another State before a recipient requests that information from their location, which may again be located on yet another State's territory.[122] In addition to regular internet traffic, a large volume of malicious forms of cyber operations manifest on and pass through the territory of States at any given time as a result of these attributes, and States routinely conduct offensive cyber operations targeting systems on the territory of other States to achieve defensive and strategic objectives.[123] Although States with the technical capabilities to do so, often in partnership with the private sector that dominates monitoring and responding to malicious cyber operations, conduct cybersecurity activities to defend against offensive cyber operations on their territory, there are no known instances of such activities being carried out by States because they consider themselves

[119] Schmitt (n 8) 31.

[120] McDonald (n 15) 1048.

[121] In *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v US*) (Merits) [1986] ICJ Rep 14, paras 154–156, recalling *Corfu Channel*, the Court stated that whether a State knew or should have known about occurrences on its territory must be established on a case-by-case basis. Also see ILA First Report (n 13) 12.

[122] As the UK acknowledges, 'common ground [among States] also extends to an appreciation that we must carefully preserve the space for perfectly legitimate everyday cyber activity which traverses multiple international boundaries millions of times a second', UK Government, 'Speech: International Law in Future Frontiers, Attorney General Suella Braverman' (*GOV.UK*, 19 May 2022) <https://www.gov.uk/government/speeches/international-law-in-future-frontiers>.

[123] See D Efrony and Y Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice' (2018) 112 AJIL 583; J Goldsmith and A Loomis, 'Defend Forward and Sovereignty' in J Goldsmith (ed), *The United States' Defend Forward Cyber Strategy* (OUP 2022) 159–5; and S Watts and T Richard, 'Baseline Territorial Sovereignty and Cyberspace' (2018) 22 LewClarkLRev 771, 837.

to be under a legal obligation of due diligence.[124] Reflecting this practical reality, assertions that States are under binding due diligence obligations in relation to cyber operations involve very particular assumptions of the content and nature of those obligations in the cyber context without any legal authority.

It took years for binding due diligence obligations to be developed in primary rules in the field of international environmental law, and it is unreasonable to seek to transpose such obligations from this—or indeed any other field—in a universal manner to cyber operations without authority or consent from States in doing so, with demonstrably contrary State practice and insufficient *opinio juris* to identify such obligations and their content. Those seeking to assert that States are under binding due diligence obligations in relation to cyber operations on their territory have attempted to bypass or circumvent State positions as reflected in consensus reports of UN fora—in this case the explicit agreement in the UN GGE defining such obligations as a voluntary non-binding norm of responsible State behaviour and the UN OEWG's clear reluctance to recognize or develop binding due diligence obligations in relation to cyber operations—by characterizing cyber operations as mere 'technological developments', to which all rules, and obligations, of international law apply by default.[125]

In 2021 Coco and Dias noted controversy over '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'.[126] However, the authors state that while 'on the one hand' the UN GGE processes failed to confirm such legal obligations existed, though the UN GGE explicitly identifying due diligence as a voluntary, non-binding norm of responsible State behaviour for cyber operations (the UN OEWG which failed to include any such language is omitted), 'on the other hand', Rule 6 of the *Tallinn Manual 2.0* states that 'a general rule or principle of this kind already exists in customary international law, and is applicable in cyberspace'.[127] The authors state that 'these views seem irreconcilable, and neither of them has gone unchallenged'.[128] However, these two opposing views are clearly not equivalent in status; indeed, such a premise unfairly implies opposing positions supported by comparable legal authority. The consensus Reports of the UN GGE explicitly

[124] See the position of Israel which touches on this issue, R Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) 97 IntlLStud 395, 404.

[125] See D Akande, A Coco and T de Souza Dias, 'Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond' (*EJIL: Talk!*, 5 January 2021) <https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/>; D Akande, A Coco and T de Souza Dias, 'Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies' (2022) 99 IntlLStud 34; Dias and Coco, *Cyber Due Diligence in International Law* (n 99) 13–57.

[126] Coco and Dias (n 6) 772. [127] ibid 773. [128] ibid 773.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

determined that such obligations were 'voluntary, non-binding norms of responsible State behaviour',[129] and the consensus Final Report of the UN OEWG failed to include any language on due diligence obligations after much deliberation on the issue, which clearly demonstrate that States do not consider themselves to be under any binding due diligence obligations in relation to cyber operations as a matter of international law. Despite their significant influence on the debate, the *Tallinn Manual* publications suffer from a particular bias both in relation to their underlying approach and the composition of their Group of Experts.[130] The 'Rules' of the *Tallinn Manual 2.0* are often cited in a manner disproportionate to their status,[131] and this is a clear example of that: a North Atlantic Treaty Organization (NATO) initiative academic publication that seeks to pursue a particular agenda in its approach and assertions surely is not equivalent to consensus reports from multiple UN processes wherein States have discussed and negotiated how international law should apply to State cyber operations over a number of decades.

Perhaps aware of the fundamental weaknesses in claiming due diligence is a general principle from which binding due diligence obligations may be universally derived for all areas of activity, and in light of the further solidified position of States in UN fora that clearly do not agree with the existence of such binding obligations for cyber operations, Coco and Dias contend that this 'current debate misses the point by focusing too much on the meaning of "due diligence" and its applicability to cyberspace', and lament these resulting 'binary, "all-or-nothing" views'.[132] However, the fact remains that States are either under legally binding due diligence obligations in relation to cyber operations on their territory, or they are not. Seeking to distinguish themselves from other positions but still recognizing their foundation in primary rules, the authors 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

[129] 2021 GGE Report (n 1) 10.

[130] See discussion in KE Eichensehr, 'Review of *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Michael N. Schmitt ed., 2013)' (2014) 108 AJIL 585.

[131] See Efrony and Shany (n 123) 585, who found only limited support in State practice for the 'rules' presented in the *Manuals*, leading them to 'question the degree to which the Tallinn Rules are universally regarded as an acceptable basis for articulating the norms of international law governing cyberoperations'.

[132] Coco and Dias (n 6) 773.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

> states to exert their best efforts in preventing, halting and redressing a variety of harms, online and offline.[133]

The benefits of States developing or recognizing due diligence obligations in cyberspace are promoted as follows:

> 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 [European Union] 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'.[134]

Note the language of 'promising route' that implies the necessary development or recognition of such obligations by States. The referenced press release made on behalf of EU Member States during the COVID-19 pandemic is not evidence or authority that due diligence obligations apply generally to any given scenario.[135] The press release neither speaks of obligations under international law, only of '[consistency] with international law' as an additional clarifying point at the end of the quoted sentence, nor does it speak for all States in such a matter.[136] A more objective and thorough examination of due diligence obligations in relation to COVID-19 determines that 'due diligence cannot be characterised as a general principle of international law due to its diverse content in different fields of international law and its dependence on accompanying primary rules'.[137]

Building on the presentation of a paper advancing these arguments in workshops in 2020,[138] the 2021 article by Coco and Dias appears to portray significant uncertainty among the authors over the existence of a 'general principle' of due diligence, again presumably in the sense of Article 38(1)(c) of the ICJ Statute, from which it is possible to derive binding obligations for all areas of activity: 'is there a general principle of due diligence in international law? Perhaps.'[139] Instead, the authors chose to rely upon an

[133] ibid 774.

[134] ibid 772.

[135] Also see related arguments made in A Coco and T de Souza Dias, 'Prevent, Respond, Cooperate: States' Due Diligence Duties vis-à- vis the COVID-19 Pandemic' (2020) 11 JIntlHumLegStud 218.

[136] 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) <https://south.euneighbours.eu/news/declaration-high-representative-josep-borrell-behalf-european-union-2/>.

[137] Peters, Krieger and Kreuzer (n 21) 121.

[138] Workshops formed part of the Oxford Process, 'The Oxford Process' (Oxford Institute for Ethics, Law and Armed Conflict) <https://www.elac.ox.ac.uk/the-oxford-process/>.

[139] Coco and Dias (n 6) 805.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

alternative 'patchwork of protective obligations' that have a purported basis in 'several primary rules of international law'.[140]

The core of their argument may be summarized as follows. First, the authors assert that 'the entirety of international law'—including 'protective' obligations—applies by default to cyberspace, 'in the absence of *leges speciales* to the contrary',[141] a claim they state is supported by State practice and *opinio juris*.[142] Second, the authors identify 'four sets of protective duties requiring states to prevent, halt or redress certain harms by behaving diligently in cyberspace',[143] where the two main sources of these obligations 'can be traced to primary obligations of general international law'.[144]

The first point, that 'the entirety of international law'—including 'protective' obligations—applies by default to cyberspace, 'in the absence of *leges speciales* to the contrary',[145] attempts to minimize the unique nature of the attributes of cyber operations and the challenges they present for the application of international law as a basis to affirm that certain rules and obligations apply to them without State practice and *opinio juris*, or indeed the consent of States. The consensus UN GGE reports explicitly recognize that challenges presented by the 'unique attributes' of cyber operations means 'additional norms could be developed over time',[146] and that 'existing norms may be formulated for application to the ICT environment … where additional norms that take into account the complexity and unique attributes of ICTs may need to be developed'.[147] The final report of the UN OEWG also adopted by consensus, recognized that 'additional norms could continue to be developed over time', and that 'the further development of norms, and the implementation of existing norms were not mutually exclusive but could take place in parallel'.[148]

It is plainly not the case from the treatment of the ICJ and sources discussed in the previous section of this article that binding due diligence obligations automatically exist universally in any and all areas of activities unless a rule exists to the contrary. This assertion is contrary to positivism and the very involvement of States and their consent in the formation and development of international law, and ignores areas of activity where binding obligations do not exist, or where soft-law obligations exist that are not binding, for example, a failure to take adequate measures to prevent the collapse of a banking system which may lead to a global financial crisis, a field in which

[140] ibid 774. [141] ibid 780. [142] ibid 778–83. [143] ibid 774, 783–804. [144] ibid 774.

[145] In relation to the basis of such arguments, see Akande, Coco and Dias, 'Old Habits Die Hard' (n 125); Akande, Coco and Dias, 'Drawing the Cyber Baseline' (n 125); Dias and Coco, *Cyber Due Diligence in International Law* (n 99) 13–57.

[146] 2013 GGE Report (n 1) 8; 2015 GGE Report (n 1) 7; 2021 GGE Report (n 1) 8.

[147] 2015 GGE Report (n 1) 7; also see UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (30 July 2010) UN Doc A/65/201, 8, which notes that '[g]iven the unique attributes of ICTs, additional norms could be developed over time' (2010 GGE Report).

[148] OEWG Final Report (n 3) 5.

only soft-law obligations exist.[149] In certain areas, soft law beyond the formal sources of Article 38 of the ICJ Statute has played a role in shaping due diligence standards; however, the interchangeable reliance on sources of international law and soft law provides yet further confusion and has been criticized as such.[150] The ICJ clearly recognizes that due diligence obligations are based in primary rules, and has explicitly cautioned against the transposition of due diligence obligations from one area of international law to another.[151] Indeed, the authors extensively detail how due diligence obligations vary across the different 'protective' obligations where they have been developed by States in relation to the circumstances and fields in which they apply.[152]

To the second point, the authors identify '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, which we call the 'Corfu Channel' principle; and (ii) states' duty to prevent and remedy significant transboundary harm, even if caused by lawful activities, known as the 'no-harm' principle. 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 or 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.[153]

However, far from a 'paradigm shift in the understanding and conceptualization of international law concerning diligent state behaviour in cyberspace',[154] this 'patchwork approach' appears to constitute only a superficial attempt to distance itself from arguments that due diligence is a general principle in international law from which it is possible to derive binding obligations across all areas of State activities, but which ultimately relies upon the same flawed basis and therefore encounters the same problems as such arguments. Namely, due diligence obligations must be contained within primary rules, and second, due diligence, or its component parts, are not primary rules from

[149] Heathcote (n 52) 299; see discussion in K Alexander, R Dhumale and J Eatwell, *Global Governance of Financial Systems: The International Regulation of Systemic Risk* (OUP 2005) 134–54. See further discussion in Section IV of this article.

[150] Peters, Krieger and Kreuzer (n 11) 11; on the status and role of soft law generally, see A Boyle and C Chinkin, *The Making of International Law* (OUP 2007) 211–29.

[151] *Prevention and Punishment of the Crime of Genocide* (n 18) para 429.

[152] Coco and Dias (n 6) 775–8.

[153] ibid 774–5.

[154] ibid 775.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

which universally binding obligations may be identified across all areas of activity. Indeed, breaking the argument of a general principle of due diligence obligations down into separate composite principles does not serve to strengthen the argument; if anything, there is even less cumulative authority in support of a so-called '*Corfu Channel* principle' and a 'no-harm principle'. Such terms have not previously been employed by international courts or in literature to denote their status as primary rules from which it is possible to derive universal binding due diligence obligations for all areas of activity.

The third and fourth 'protective duties' are also misleading as they introduce other specific areas where due diligence obligations would be anchored in primary rules in an attempt to strengthen these general underlying normative 'patchwork' claims in the cyber context. The human rights context mirrors complications concerning the application of international law to cyberspace more broadly: the consequences of challenges presented by the unique nature of cyber operations result in the 'radical reinterpretation of existing human rights norms, the emergence of new digital human rights, and the extension of human rights law to new right-holders and duty-holders', where 'developments relating to digital human rights are also contributing to, and are influenced by, broader changes in IHRL [international human rights law]' including 'the [ongoing] expansion of positive obligations relating to the conduct of private companies'.[155] While international humanitarian law faces similar normative issues in relation to the challenges presented by the unique nature of cyber operations, their scope is limited in that the vast majority of cyber operations consist of low-level intrusions that take place outside of armed conflict, where international humanitarian law is not implicated. Furthermore, actions undertaken by States that are performed for non-legal reasons in this area should not be taken as evidence of an overarching obligation,[156] and to the extent that due diligence obligations exist they would be more properly characterized as part of individual primary rules of international law.[157] In any case, the development or existence of binding obligations in these areas has no bearing on the claim that due diligence (or composite principles of due diligence) is a universal standalone source from which it is possible to derive binding obligations for all areas of activity. This conflation with obligations of conduct in other areas of law is particularly apparent in the recent positions of Costa Rica and Ireland, which appear to have been influenced by these arguments in citing the application

[155] Y Shany, 'Digital Rights and the Outer Limits of International Human Rights Law' (2023) 24 GermLJ 461, 471.

[156] See McDonald (n 15) 1049–54.

[157] H Moynihan, 'Aiding and Assisting: Challenges in Armed Conflict and Counterterrorism' (2016) Chatham House, International Law Programme Research Paper, 15 <https://www.chathamhouse.org/sites/default/files/publications/research/2016-11-11-aiding-assisting-challenges-armed-conflict-moynihan.pdf>.

of due diligence obligations in international human rights law and international humanitarian law.[158]

Ultimately, like preceding attempts to identify binding due diligence obligations for cyber operations based upon construing due diligence as a general principle, the heavy lifting of these assertions rests on a fundamental misrepresentation of the *Corfu Channel* judgment (the 'Corfu Channel principle') and the traditional no-harm rule established in the field of international environmental law. The assertion that binding obligations for all areas of activity may be identified from a 'Corfu Channel principle' and a 'no-harm principle' are wholly at odds with the status and function of due diligence obligations and the treatment of such obligations by the ICJ as examined in the second part of this article, and the authors are unable to provide any authority beyond the *Tallinn Manual 2.0* and like-minded cyber-specific literature in support of these assertions.

Notably, the legal obligation in *Corfu Channel* emanated from primary rules of international law in relation to that discrete context, specifically, the right of innocent passage and the concomitant obligation of the coastal States not to hamper this right.[159] The Court's conclusion was that 'it is only in relation to established rights that an obligation of due diligence is owed by one State to another (in the *Corfu Channel* case, the right of innocent passage)'.[160] In this manner, it was the finding of the Court on innocent passage that was crucial for the outcome of the case.[161] This is consistent with the ICJ's treatment of due diligence obligations in later cases which underlines that they must be anchored in a primary rule in order to arise,[162] and the Court's explicit caution against the transposition of due diligence obligations from one area of international law to another.[163]

The attempt to broaden the application of the customary no-harm rule developed in international environmental law to cyberspace is problematic because of these same reasons: in order to make such an argument, it is necessary both to misrepresent the character of the no-harm principle in international environmental law as possessing a far broader application, and to contradict the contrary treatment of such obligations in ICJ case law by claiming that such a universal standalone source exists from which it is possible to derive binding obligations for all areas of activity due to insufficient State practice and *opinio juris* in support of a customary rule for

[158] Ministry of Foreign Affairs of Costa Rica, 'Costa Rica's Position on the Application of International Law in Cyberspace' (21 July 2023) 9 <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf>; Irish Department of Foreign Affairs, 'Ireland: Position Paper on the Application of International Law in Cyberspace' (6 July 2023) para 12 <https://www.dfa.ie/media/dfa/ourrolepolicies/internationallaw/Ireland---National-Position-Paper.pdf>. [159] *Corfu Channel* (n 18) 10. [160] Heathcote (n 52) 299.
[161] Waibel (n 49); Ollino (n 41) 54. [162] See analysis in Section II of this article.
[163] *Prevention and Punishment of the Crime of Genocide* (n 18) para 429.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

cyberspace.[164] However, even tracing the no-harm rule back to before the ICJ's treatment of due diligence obligations does not provide support for such an argument, where the statement of law relating to due diligence was addressed by international tribunals in *Spanish Zone*,[165] *Island of Palmas*[166] and *Trail Smelter*.[167] In 1925, in the *Spanish Zone* case, Max Huber stated that '[t]he responsibility for events which may affect international law and which occur in a given territory goes hand in hand with the right to exercise, to the exclusion of other States, the prerogatives of sovereignty'.[168] Similarly, in the 1928 *Island of Palmas* Award Huber stated that by virtue of their territorial sovereignty States have 'the obligation to protect within the territory the rights of other States'.[169] Finally, in the *Trail Smelter* Award the tribunal stated that:

> … under the principles of international law, as well as of the law of the United States, no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of serious consequence and the injury is established by clear and convincing evidence.[170]

This statement from *Trail Smelter*, along with the *Corfu Channel* case, is considered to form the cornerstone of international environmental law as reiterated in ICJ cases that followed. In its Advisory Opinion on the *Legality of the Threat or Use of Nuclear Weapons*, the ICJ affirmed for the first time that customary obligations had developed within international environmental law:

> The existence of the general obligation of States to ensure that activities within their jurisdiction and control respect the environment of other states or of areas beyond national control is now *part of the corpus of international law relating to the environment*.[171]

The status of this customary rule was clearly established in international environmental law, as affirmed by subsequent case law.[172] In light of the ICJ's recognition that due diligence obligations are based in primary rules and explicit cautioning against the transposition of due diligence obligations from one area of international law to another,[173] binding obligations do not

[164] eg, see Lahmann who cites *Pulp Mills* to assert a positive duty to prevent exists as a customary rule that is applicable in the cyber context, H Lahmann, *Unilateral Remedies to Cyber Operations* (CUP 2020) 147.

[165] *British Claims in the Spanish Zone of Morocco Case* (1 May 1925) 2 UNRIAA 615, 649.

[166] *Island of Palmas Case* (*Netherlands v USA*) (4 April 1928) 2 UNRIAA 829, 839.

[167] *Trail Smelter* (n 46) 1965.

[168] *British Claims in the Spanish Zone* (n 165) 649; English translation: 'Report of the International Law Commission on its 31st Session' (1979) II(2) ILC Ybk 98, fn 505.

[169] *Island of Palmas* (n 166) 839.

[170] *Trail Smelter* (n 46) 1965.

[171] *Legality of the Threat or Use of Nuclear Weapons* [1996] ICJ Rep 226, para 29 (emphasis added).

[172] Reiterated in *Gabčíkovo-Nagymaros* (n 47) para 53; and more recently in *Pulp Mills* (n 18) para 193.

[173] *Prevention and Punishment of the Crime of Genocide* (n 18) para 429.

automatically extend to activity in cyberspace. Even within the context of international environmental law where this rule crystallized,[174] '[c]ertainly not all instances of transboundary damage resulting from activities within a State's territory can be prevented or are unlawful'.[175] Beyond the above quoted statements in *Spanish Zone*, *Island of Palmas* and *Trail Smelter* that may be understood to constitute 'really no more than statements of what sovereignty means',[176] many arbitral awards prior to *Corfu Channel* also applied specific primary rules of due diligence relating to the protection of aliens and foreign State representatives.[177] Furthermore, the approach of the Court in *Corfu Channel* provides an additional demonstration that due diligence obligations are anchored in primary rules: the Hague Convention VIII of 1907 Relative to the Laying of Automatic Submarine Contact Mines was, contrary to UK pleadings, not held to be applicable because it was restricted to times of war.[178]

Ollino summarizes the significance of *Corfu Channel* and *Pulp Mills* as follows:

> In the Corfu Channel case, the ICJ judges inferred Albania's duty to exercise due diligence by way of notification from a combination of established rights (the right of innocent passage) and obligations (the *alienum non laedas* obligation). In Pulp Mills, the court appeared to invoke due diligence as a shorthand expression for identifying the no-harm rule and the underlying *nature* of the conduct that this obligation imposes on states. *Both in the Corfu Channel and Pulp Mills decisions, the duty to exercise due diligence was indeed highly contextualised and construed in relation to the general principles and obligations (the primary rules) to which it applied.*[179]

Influenced by these assertions seeking to identify binding obligations in cyberspace, an increasing number of mostly European States have released statements on the application of international law to cyber operations that may be considered to provide support for due diligence obligations for cyber operations based upon these misrepresentations of the status and function of due diligence.[180] However, even States that endorse a binding rule of due

[174] For further context also see the wording of principle 2 of the 1992 Rio Declaration on Environment and Development (n 29), which essentially reaffirms principle 21 of the Stockholm Declaration (The United Nations Conference on the Human Environment held in Stockholm, June 1972) <https://wedocs.unep.org/bitstream/handle/20.500.11822/29567/ELGP1StockD.pdf>.

[175] UN Economic and Social Council, 'Report of the Secretary-General: Rio Declaration on Environment and Development: Application and Implementation' (10 February 1997) UN Doc E/CN.17/1997/8, para 23.

[176] Heathcote (n 52) 298.

[177] See R Ago, 'Fourth Report on State Responsibility' (1972) II ILC Ybk, 100–6, paras 74–90; concerning foreign State representatives, see R Ago, 'Seventh Report on State Responsibility' (1978) I(1) ILC Ybk, 35, para 13, fn 18.

[178] *Corfu Channel* (n 18) 22.

[179] Ollino (n 41) 54–5 (emphasis added).

[180] Including Ministry of Foreign Affairs of Costa Rica (n 158) 8–9; the Czech Republic, 'Special Envoy of Czech Republic for Cyberspace, Director of Cybersecurity Department, Statement Dated 11 February 2020, from the Special Envoy of Czech Republic for Cyberspace, Director of Cybersecurity Department at the 2nd Substantive Session of the Open-Ended Working Group on

diligence for cyber operations recognize clear disagreement over its existence and application,[181] or express the expectation that such obligations will develop and crystallize over time.[182] These States also maintain significant differences on what the content of such obligations should entail in cyberspace, in particular in relation to the level of knowledge that a State is required to have, the types of activity a State is required to carry out in accordance with their legal obligation, and the seriousness of the harm caused by the malicious cyber activity on the territory.[183] In practice, *opinio juris* is often difficult to ascertain because in their behaviour States may or may not be wilfully pursuing the objective of contributing to the creation, the modification, or the termination of a customary rule.[184] As such, in expressing views as to whether certain behaviours are legally obligatory or as to whether a particular rule of customary law exists, it is challenging to differentiate real expressions of belief

Developments in the Field of Information and Telecommunications in the Context of International Security of the First Committee of the General Assembly of the United Nations' (2nd substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security' (11 February 2020) <https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf>; Denmark, 'Denmark's Position Paper on the Application of International Law in Cyberspace: Introduction' (2023) NordicJIL 1, 7–8; Estonia, UNGA, UN Doc A/76/136 (n 98) 26; France, 'International Law Applied to Operations in Cyberspace' (2021) 6, 9–10 <https://web.archive.org/web/20220307043619/https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf>; Germany, The Federal Government, 'On the Application of International Law in Cyberspace' (March 2021) 3, 11 <https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf>; Ireland, Irish Department of Foreign Affairs (n 158) 3–4; Italy, 'Italian Position Paper on "International Law and Cyberspace"' (2021) 6–7 <https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf>; Japan takes a somewhat ambiguous position, Ministry of Foreign Affairs of Japan (n 98) 5; the Netherlands, though the position acknowledges that 'not all countries agree that the due diligence principle constitutes an obligation in its own right under international law', Government of the Netherlands, 'Appendix: International Law in Cyberspace, Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace, Translation' (26 September 2019) 4–5 <https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>; Norway, UNGA, UN Doc A/76/136 (n 98) 71–2; Romania, though note the proposal of cyber-specific 'elements [that must be] cumulatively met' for such obligations to arise, ibid 76 (2021); Sweden, Government Offices of Sweden, 'Position Paper on the Application of International Law in Cyberspace' (July 2022) 4–5 <https://www.government.se/contentassets/3c2cb6febd0e4ab0bd542f653283b140/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf>; and Switzerland, Federal Department of Foreign Affairs, 'Switzerland's Position Paper on the Application of International Law in Cyberspace' (2021) 7 <https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf>.

[181] eg, see positions of Japan, UNGA, UN Doc A/76/136 (n 98) 48; and the Netherlands, ibid 58; see discussion in KE Eichensehr, 'Not Illegal: The SolarWinds Incident and International Law' (2022) 33 EJIL 1263.

[182] eg, see the position of Denmark (n 180) 8.

[183] See discussion in part III of H Moynihan, 'Unpacking Due Diligence in Cyberspace' (2023) 8 JCyberPol <https://doi.org/10.1080/23738871.2023.2250358>.

[184] T Treves, 'Customary International Law' in R Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (OUP 2006).

(manifestations of *opinio juris*), from acts made with the purpose of influencing the formation, the modification or the termination of a customary rule.

In reaction to these claims, other States have expressed more accurate understandings of the status of due diligence obligations reflected in sources of international law, with some reasonably reiterating that references to due diligence activities in UN GGE Reports, adopted by consensus, were explicitly defined as voluntary, non-binding norms of responsible State behaviour:[185] namely, that such obligations develop as part of primary rules in particular contexts, and there is currently insufficient State practice and *opinio juris* for such a primary rule to crystallize containing binding due diligence obligations that apply to cyber operations.

Others have generally called for due diligence obligations to be developed if they are to become established[186] or make statements featuring non-mandatory language that are consistent with due diligence in relation to cyber operations as a voluntary non-binding norm of responsible State behaviour as reflected by State positions in UN fora consensus reports.[187] Notably, States with the most advanced cyber capabilities do not recognize binding due diligence obligations in relation to cyber operations.[188] Reports by Hollis for the Organization of American States on international law and State cyber

[185] eg, see the position of Argentina, Argentina, statement at the Second Substantive Session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (UN, 11 February 2020) <https://media.un.org/en/asset/k18/k18w6jq6eg>; the US, UNGA, UN Doc A/76/136 (n 98) 141; the UK, Foreign, Commonwealth & Development Office, 'Application of International Law to States' Conduct in Cyberspace: UK Statement' (3 June 2021) <https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement>; New Zealand, New Zealand Ministry of Foreign Affairs and Trade, 'The Application of International Law to State Activity in Cyberspace' (1 December 2020) <https://www.mfat.govt.nz/en/media-and-resources/the-application-of-international-law-to-state-activity-in-cyberspace/>; and Israel, Schöndorf (n 124) 404 (2020).

[186] eg, see the position of Singapore: 'There is a need for more clarity on the scope and practical applications, if any, of due diligence in cyberspace.' UNGA, UN Doc A/76/136 (n 98) 84.

[187] eg, see the position of Australia, Australian Government, 'Annex B: Australia's Position on How International Law Applies to State Conduct in Cyberspace, Australia's International Cyber and Critical Tech Engagement' (2020) <https://www.internationalcybertech.gov.au/our-work/annexes/annex-b>; Canada, Government of Canada, 'International Law Applicable in Cyberspace' (22 April 2022) <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng>; China states generally that '[n]o State shall knowingly allow its territory, or territory or ICT facilities, data and information under the control of its government, to be used for ICT activities that undermine national security or interests', 'China's Views on the Application of the Principle of Sovereignty in Cyberspace' (2021) 1–2 <https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf>; Poland, 'The Republic of Poland's Position on the Application of International Law in Cyberspace' (2022) 4 <https://www.gov.pl/attachment/3203b18b-a83f-4b92-8da2-fa0e3b449131>; see the consensus position of States in the 2021 GGE Report (n 1) 8; and 2015 GGE Report (n 1) 7, 8.

[188] For an assessment of State cyber capabilities, see J Voo, I Hemani and D Cassidy, 'National Cyber Power Index 2022' (Belfer Center for Science and International Affairs 2022) <https://www.belfercenter.org/publication/national-cyber-power-index-2022>.

operations which directly solicited State views on whether due diligence '[qualifies] as a rule of international law that States must follow' in cyberspace determined that 'at the global level there is no universal consensus among States on what existing general international laws apply to cyber operations, let alone how they do so', noting reluctance, 'outstanding controversy and confusion on whether certain existing international legal regimes apply to cyber operations, including … due diligence'.[189] Furthermore, there are sparse instances where States have invoked the language of international law to activities in cyberspace generally,[190] and no examples of State actions in cyberspace have been reported to have been performed in compliance with a legal due diligence obligation.

Israel explains the clear and deliberate reasoning behind the explicit and consensus agreement among States—including the permanent five members of the Security Council—to use language of 'non-binding and voluntary' (that was also expressed by other States) in the UN GGE Reports, following an approach compatible with the Court's position in the *Prevention and Punishment of the Crime of Genocide* in cautioning against applying rules developed in different contexts,[191] to cyberspace:

> In the 2015 UN GGE Report, the concept [of due diligence] was addressed as the basis for a voluntary, non-binding norm of responsible State behavior, providing that States should not allow their territory to be used for the commission of international wrongful acts. *There was wisdom in mentioning it in the chapter covering norms of responsible State behavior, as it does not, at this point in time, translate into a binding rule of international law in the cyber context. This was the position expressed by other States as well.*
>
> … we have to be careful in applying to the cyber domain rules that emerged in a different, distinct context …
>
> … we have not seen widespread State practice beyond this type of voluntary cooperation, and certainly not practice grounded in some overarching *opinio juris*, which would be indispensable for a customary rule of due diligence, or something similar to that, to form.[192]

New Zealand takes a similar position and states that due diligence obligations in relation to cyber operations are yet to crystallize (into a primary rule of customary international law):

[189] DB Hollis, 'Improving Transparency: International Law and State Cyber Operations: Fifth Report' (Inter-American Juridical Committee 2020) 7, para 5 <http://www.oas.org/en/sla/iajc/docs/International_Law_and_State_Cyber_Operations_publication.pdf>, citing Hollis (n 91); DB Hollis, 'Improving Transparency: International Law and State Cyber Operations: Fourth Report' (5 March 2020) OEA/Ser.Q, CJI/doc. 603/20 rev.1 corr.1, 1 <https://www.oas.org/en/sla/iajc/docs/CJI_doc_603-20_rev1_corr1_eng.pdf>.

[190] DB Hollis, 'Improving Transparency: International Law and State Cyber Operations – Fifth Report' (7 August 2020) OEA/Ser.Q, CJI/doc. 615/20 rev.1, 2 <https://www.oas.org/en/sla/iajc/docs/CJI-doc_615-20_rev1_ENG.pdf>; Efrony and Shany (n 123) 586.

[191] *Prevention and Punishment of the Crime of Genocide* (n 18) para 429.

[192] Schöndorf (n 124) 404 (emphasis added).

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

> An agreed norm of responsible state behaviour provides that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. Whether this norm also reflects a binding legal obligation is not settled …
>
> New Zealand is not yet convinced that a cyber-specific 'due diligence' obligation has crystallised in international law. It is clear that states are not obliged to monitor all cyber activities on their territories or to prevent all malicious use of cyber infrastructure within their borders. If a legally binding due diligence obligation were to apply to cyber activities, New Zealand considers it should apply only where states have actual, rather than constructive, knowledge of the malicious activity, and should only require states to take reasonable steps within their capacity to bring the activity to an end.[193]

The UK further highlights the clear language of the 2021 UN GGE Report which explicitly defines due diligence obligations as a non-binding and voluntary norm of responsible State behaviour:

> UNGGE Norm 13(c) provides that States should not knowingly allow their territory to be used for internationally wrongful acts using information and communications technology. This norm provides guidance on what may be expected to constitute appropriate State behaviour … *the fact that States have referred to this as a non-binding norm indicates that there is not yet State practice sufficient to establish a specific customary international law rule of 'due diligence' applicable to activities in cyberspace.*[194]

The US adopts a similar position, citing the lack of State practice and *opinio juris* in relation to assertions of due diligence as a general obligation under international law in relation to cyber operations:

> In recent public statements on how international law applies in cyberspace, a few States have referenced the concept of 'due diligence': that States have a general international law obligation to take steps to address activity emanating from their territory that is harmful to other States, and that such a general obligation applies more specifically, as a matter of international law, to cyber activities. The United States has not identified the State practice and opinio juris that would support a claim that due diligence currently constitutes a general obligation under international law.[195]

Argentina has asserted that 'under international law, there is no obligation of due diligence when it comes to cybersecurity'.[196] The Russian Federation provides further evidence that States do not consider themselves to be under binding due diligence obligations, explicitly questioning the 'automatic' extrapolation of international law to cyber operations and proposing the

[193] New Zealand Ministry of Foreign Affairs and Trade (n 185) paras 16, 17.
[194] UK Foreign, Commonwealth & Development Office (n 185) (emphasis added).
[195] UNGA, UN Doc A/76/136 (n 98) 141.
[196] Argentina, statement at the Second Substantive Session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (UN, 11 February 2020) <https://media.un.org/en/asset/k18/k18w6jq6eg>.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

drafting of an international treaty[197] that has received significant support among States, establishing a UN process to draft a global 'cybercrime' treaty to govern cyber operations.[198]

Even the Cyber Law Toolkit, a website affiliated with the same body responsible for creating the *Tallinn Manual* projects, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE), that maintains a collection of State positions on matters of international law related to cyber operations, currently acknowledges that '[i]t is the matter of some controversy whether the principle of due diligence reflects a binding obligation applicable to cyber operations'.[199]

In the *North Sea Continental Shelf* cases the ICJ stated that State practice must be 'both extensive and virtually uniform', and that it must include the practice 'of States whose interests are specially affected'.[200] While States that possess relatively modest or undeveloped cyber capabilities have yet to contribute to State practice through conducting operations in a manner that is easily identifiable from publicly available information, it is possible to identify a common trend of offensive practice in States conducting cyber operations which target systems on the territory of foreign States among those that possess the capabilities to conduct such operations.[201] The US ('defend forward'),[202] the UK ('active defence'),[203] Canada ('active cyber'),[204] New Zealand ('internationally active' engagement)[205] and Australia ('deter and respond')[206] are examples of States that recognize the

[197] UNGA, UN Doc A/76/136 (n 98) 80.

[198] In 2019 the UNGA adopted a resolution by 79 votes to 60 with 33 abstentions to establish an Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes; see UNGA Res 74/247 (20 January 2020) UN Doc A/RES/74/247.

[199] 'Due Diligence' (*International Cyber Law: Interactive Toolkit*, 5 May 2022) <https://cyberlaw.ccdcoe.org/wiki/Due_diligence>.

[200] *North Sea Continental Shelf cases (Federal Republic of Germany/Denmark; Federal Republic of Germany/Netherlands)* (Judgment) [1969] ICJ Rep 3, para 74.

[201] See Efrony and Shany (n 123) 585; Goldsmith and Loomis (n 123) 159–65; Watts and Richard (n 123) 837.

[202] US Department of Defense, *Summary Department of Defense Cyber Strategy 2018* (2018) 1 <https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF>; on the implications of 'defend forward' for Rule 4 of the *Tallinn Manual 2.0*, see Goldsmith and Loomis (n 123).

[203] HM Government, *National Cyber Security Strategy 2016–2021* (2016) 33–5 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf>.

[204] Parliament of Canada, 'Government Bill (House of Commons) C-59 (42-1) (Third Reading): An Act Respecting National Security Matters' (19 June 2018) section 19 <https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/third-reading#enH3105>.

[205] New Zealand Government, *New Zealand's Cyber Security Strategy 2019* (Department of the Prime Minister and Cabinet 2019) 13 <https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf>.

[206] Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy* (October 2017) 54 <https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf>.

routine conduct of low-level cyber operations in official policy documents. These States clearly consider such operations to be in full compliance with their obligations under international law.[207] Furthermore, even States that endorse the recognition of binding due diligence obligations in cyberspace, such as France and the Netherlands, carry out offensive cyber operations on the territory of other States that may implicate such obligations of conduct.[208]

IV. RISKS OF CONSTRUING DUE DILIGENCE AS UNIVERSAL STANDALONE SOURCE

Beyond the inherent difficulties in supporting such claims, there are many reasons why assertions that due diligence should be treated as a universal standalone source from which it is possible to identify binding obligations across all areas of activity create significant risks and are ill advised. Specifically, there are risks that such assertions will serve to dilute substantive obligations and undermine the effectiveness and legitimacy of international law.

The effective function of due diligence obligations requires development as a procedure in any particular context, where reliance on a general concept of due diligence invoked as a 'buzzword' that has not been fleshed out to account for those attributes risks powerful States defining what is 'due' in their best interests.[209] Attempts to frame due diligence as a universal standalone source in this manner as a broad (indeterminate) normative standard may 'undermine the capacity of the law to govern behaviour, because the vague and blurry terms of those norms give plenty of leeway to those interpreting and applying them', '[undermining] the international rule of law'.[210] Furthermore, the introduction of due diligence obligations where treaty regimes previously provided substantive standards may serve to dilute the strictness of such standards by introducing State discretion.[211]

In the context of State cyber operations, some States such as Russia and China refer to the principle of sovereignty in relation to concerns over national security in an effort to justify restrictions on access to information

[207] eg, the US Department of Defense states that 'The Department's commitment to defend forward including to counter foreign cyber activity targeting the United States—comports with our obligations under international law and our commitment to the rules-based international order', Hon PC Ney, Jr, 'DOD General Counsel Remarks at U.S. Cyber Command Legal Conference' (U.S. Department of Defense, 2 March 2020) <https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/>.

[208] See J Kenny, 'France, Cyber Operations and Sovereignty: The "Purist" Approach to Sovereignty and Contradictory State Practice' (*Lawfare*, 12 March 2021) <https://www.lawfareblog.com/france-cyber-operations-and-sovereignty-purist-approach-sovereignty-and-contradictory-state-practice>.

[209] See Peters et al, 'There is the danger that States and other international persons simply proclaim due diligence and then do what they want', Peters, Krieger and Kreuzer (n 21) 134.

[210] ibid.

[211] ibid.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

and restrictions upon free speech and expression online.[212] Without development in relation to the unique attributes of cyberspace, a broad duty to monitor and prevent harmful activities in cyberspace may be used to legitimize such restrictions and even to disregard human rights violations, and may also offer further justifications in relation to disproportionate State surveillance programmes,[213] for example, the widespread mass-surveillance programmes conducted by the US.[214] At the same time, the further one goes in identifying the specific content of such obligations in prescribing appropriate measures tailored to the unique characteristics of cyberspace—for instance, suggesting States must establish certain technical bodies that perform particular cyber-related monitoring tasks—the harder it is to maintain that such content is possible to extrapolate through a process of 'interpretation' from a universal standalone source of due diligence from which it is claimed it is possible to derive binding obligations for all areas of activity without State consent.[215] Additionally, in the context of States undertaking activities as a matter of policy outside of legal obligations, such as activities related to cybersecurity, it is important to recognize that 'pushing for a "general principle of due diligence" in international law … risks having a chilling effect on this positive legal/policy "due diligence" behaviour by States'.[216] In addition to their remote, prolific and continuous nature, monitoring and response to malicious cyber operations is almost exclusively carried out by companies in the private sector. As Israel notes:

> The inherently different features of cyberspace—its decentralization and private characteristics—incentivize cooperation between States on a voluntary basis, such as with the case of national Computer Emergency Response Teams (CERTs). CERTs are already doing what could arguably fall into that category: exchanging information with one another, as well as cooperating with each other in mitigating incidents [where this practice is voluntary and not grounded in *opinio juris*].[217]

A further consideration for States in deciding whether to develop binding due diligence obligations in cyberspace relates to the debate led by the editors of the *Tallinn Manual 2.0* that promotes a 'rule' of sovereignty in cyberspace based on

[212] The International Code of Conduct for Information Security (2011) may be considered as an attempt to legitimize restrictions of free speech that disregard international human rights obligations; UNGA, 'Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General' (14 September 2011) UN Doc A/66/359; Section (c) of the Code of Conduct.

[213] 'This may give room for more self-selected processes and self-biased national narratives and thereby contribute to an alienation and even disengagement of States from their international legal commitments', Peters, Krieger and Kreuzer (n 21) 135, 134–5.

[214] See E MacAskill et al, 'NSA Files *Decoded*: Edward Snowden's Surveillance Revelations Explained' *The Guardian* (London, 1 November 2013) <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>.

[215] For a general discussion of policy implications in this context, see Moynihan (n 183).

[216] McDonald (n 15) 1041.

[217] Schöndorf (n 124) 404.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

Rule 4 of the *Manual*.[218] States that do not recognize a 'rule' of sovereignty enjoy the operational freedom to conduct operations to defend and deter malicious cyber operations emanating from the territory of another State at its source (below the threshold of use of force and prohibited intervention). It would be reasonable to assume that States that acknowledge conducting offensive cyber operations to achieve defensive and strategic objectives consider that they currently provide a more efficient and effective means of addressing threats emanating from the territory of another State than forming specific binding due diligence obligations whose breach may give rise to the possibility to invoke countermeasures in limited circumstances where capabilities and response times are critical. States enjoy various means by which to engage in unfriendly acts and retorsion below the threshold of international wrongfulness.[219] Indeed, part of the reluctance of States in recognizing a 'rule' of sovereignty in cyberspace relates to concerns over limiting the freedom to conduct precisely these kinds of operations.[220] Furthermore, some States have expressed concern about the possibility of invoking countermeasures in cyberspace and it has been suggested that countermeasures may risk escalating disputes between States, especially where States maintain such divergent views over the existence of rules and their application in cyberspace.[221]

Even if one ignores the many flaws raised by such assertions and assumes the premise that due diligence obligations are a freestanding source from which it is possible to derive binding obligations for all areas of activity, it is unclear how that argument is reconcilable with the many areas of activity where it is accepted that only soft-law non-binding obligations exist. Examples include failure to

[218] See M Schmitt and L Vihul, 'Respect for Sovereignty in Cyberspace' (2017) 95 TexLRev 1639; based on Rule 4 of the Tallinn Manual 2.0, Schmitt (n 8) 17–27; see further discussion of 'sovereignty as a rule' in M Schmitt, 'Finland Sets Out Key Positions on International Cyber Law' (*Just Security*, 27 October 2020) <https://www.justsecurity.org/73061/finland-sets-out-key-positions-on-international-cyber-law/>; and M Schmitt, 'The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis' (*Just Security*, 14 October 2019) <https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/>; for an objective analysis of these claims, see Goldsmith and Loomis (n 123).

[219] See N McDonald and A McLeod, '"Antisocial Behaviour, Unfriendly Relations": Assessing the Contemporary Value of the Categories of Unfriendly Acts and Retorsion in International Law' (2021) 26 JC&SL 421.

[220] See Efrony and Shany (n 123) 588; H Moynihan, 'The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace' (2021) 6 JCyberPol 394, 402.

[221] eg, see the positions of Brazil, UNGA, UN Doc A/76/136 (n 98) 21–2; China, Permanent Mission of the People's Republic of China, 'Statement by Counsellor SUN Lei of the Chinese Delegation at the Thematic Discussion on Information and Cyber Security at the First Committee of the 72nd Session of the UNGA' (23 October 2017) <http://un.china-mission.gov.cn/eng/chinaandun/disarmament_armscontrol/unga/201710/t20171030_8412335.htm>; and Cuba, 'Declaration by Miguel Rodríguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (23 June 2017) <https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf>; E Jensen and S Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?' (2017) 95 TexLRev 23, 1555, 1573–4.

take adequate measures to prevent the collapse of a banking system which may lead to a global financial crisis,[222] harmful transmissions or broadcasts emanating from State territories,[223] or in the area of business and human rights where for decades scholars and NGOs have sought to promote the 'hardening' of soft law by developing binding due diligence obligations in primary rules and domestic law,[224] and in relation to similar campaigns concerning human rights due diligence obligations.[225] Indeed, States would surely be shocked to learn of the sudden existence of binding due diligence obligations in *all* areas of activity on their territories where previously only soft law existed without their consent. It would remain a mystery why States went to such great lengths in forming specific primary rules containing due diligence obligations for certain areas of activity in the first place, and why they have not relied on such universal obligations rather than specific primary rules in cases before the ICJ. Similarly, the current intergovernmental working group at the UN producing the draft of a new legally binding instrument on business and human rights[226] would be relieved to learn that such obligations already exist. These examples demonstrate the absurdity of such arguments and the clear detachment this scholarship has to the reality of the status of due diligence obligations in international law. Due consideration does not appear to have been given to implications of these assertions outside the narrow confines of cyber operations, where they would effectively constitute a radical transformation of the international rules-based system, fundamentally altering the obligations of States under international law. For example, take the position of Romania which follows the unsound assertions addressed critically by this article:

> The due diligence principle entails that a State may be responsible for the effects of the conduct of private persons, if it failed to take necessary measures to prevent those effects.
>
> This principle (which implies a certain obligation of conduct on the part of States) was enunciated by the ICJ in its Corfu Channel judgment emphasizing that every State is under an 'obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'.[227]

The consequences of recognizing such an overarching broad universal standalone source of due diligence from which binding obligations derive

[222] Heathcote (n 52) 299; see discussion in Alexander, Dhumale and Eatwell (n 149) 134–54.
[223] See B Baade, 'Fake News and International Law' (2018) 29 EJIL 1357, 1365.
[224] See J Ruggie, C Rees and R Davis, 'Ten Years After: From UN Guiding Principles to Multi-Fiduciary Obligations' (2021) 6 BHRJ 179.
[225] See C Macchi and C Bright, 'Hardening Soft Law: The Implementation of Human Rights Due Diligence Requirements in Domestic Legislation' in M Buscemi et al (eds), *Legal Sources in Business and Human Rights: Evolving Dynamics in International and European Law* (Brill 2020).
[226] UN Human Rights Council Open-ended Intergovernmental Working Group (OEIGWG), 'Third Revised Draft of the Legally Binding Instrument to Regulate, in International Human Rights Law, the Activities of Transnational Corporations and other Business Enterprises' (17 August 2021) <https://www.ohchr.org/en/hr-bodies/hrc/wg-trans-corp/igwg-on-tnc>.
[227] UNGA, UN Doc A/76/136 (n 98) 76.

that apply to all areas of activity (including cyberspace), encompassing the conduct of private persons, is extraordinary and contrary to the many areas of activity where only soft law exists: do we then assume that Romania considers itself and others to be under binding obligations for all areas of activity including the conduct of non-State actors, for instance, the activities of corporations concerning the area of business and human rights?

Finally, concerns have been raised that a normative consideration against establishing due diligence as a general principle would be that 'it would not be adequate as a fallback rule'.[228] According to Peters, Krieger and Kreuzer, '[t]urning the due diligence standard into an overarching obligation to behave diligently in international relations would imply that due diligence is normatively more desirable than other standards (such as absolute harm prevention on the one side or mere avoidance of gross recklessness on the other side) [that] would create an additional legal argumentative burden for States when they intend to apply a different liability standard [and] restrict the States' freedom to work out the most appropriate allocation of accountability'.[229]

V. CONCLUSION

Contrary to assertions advanced in scholarship claiming that due diligence is a standalone universal source from which binding obligations may be derived for all areas of activity, States have developed binding due diligence obligations in particular areas of activity encompassed within primary rules tailored to those discrete contexts. The ICJ's treatment of due diligence obligations clearly underlines that they must be anchored in a primary rule in order to arise and that the nature of a legal obligation to act with due diligence is specific to a particular context. Indeed, the Court has explicitly cautioned against the transposition of due diligence obligations from one area of international law to another, recognizing that similar 'obligations to prevent' exist in various treaties but that the content of the obligations to act with due diligence was not comparable between treaty regimes and different rules of customary international law.[230]

There is currently insufficient State practice and *opinio juris* to support the crystallization of a rule of customary international law containing binding due diligence obligations in cyberspace. Indeed, there is a significant body of offensive State practice of cyber operations targeting systems on the territory of foreign States that is inconsistent with the existence of a primary rule containing binding due diligence obligations in cyberspace.[231] Furthermore,

[228] Peters, Krieger and Kreuzer (n 21) 133–4.
[229] ibid.
[230] *Prevention and Punishment of the Crime of Genocide* (n 18) para 429.
[231] See Efrony and Shany (n 123); Goldsmith and Loomis (n 123); and Watts and Richard (n 123) 837.

https://doi.org/10.1017/S0020589323000489 Published online by Cambridge University Press

there is no known practice of States taking action in compliance with a legal obligation to do so in relation to cyber operations emanating from their territory. Consensus reports of the UN GGE explicitly define due diligence obligations in relation to cyber operations as a 'non-binding voluntary norm of responsible State behaviour', and the UN OEWG was unable to agree on the inclusion of any language relating to due diligence obligations at all, even in a non-binding context. While some commentators have sought to encourage the recognition or development of binding due diligence obligations in relation to cyber operations, others have made unprecedented assertions that States are already under such obligations by construing due diligence as a universal standalone source from which it is possible to derive binding obligations applicable to all areas of activity based primarily on a misrepresentation of the ICJ's *Corfu Channel* judgment.

An increasing number of mostly European States have since supported these ambitious assertions and encouraged the development of such obligations for activity in cyberspace, though even States that endorse binding due diligence obligations in cyberspace recognize clear disagreement over their existence and application. In response, other States have expressed more accurate understandings of the status of due diligence obligations in international law, arguing that there is currently insufficient State practice and *opinio juris* to establish a specific customary international law rule of 'due diligence' applicable to cyber operations. Some of these States have referred to the deliberate explicit definition of due diligence as a non-binding norm of responsible State behaviour in consensus UN GGE Reports after extensive discussion of such issues, which reflects that States do not consider themselves to be under any binding due diligence obligations in relation to cyber operations. If anything, the position of States in UN fora serves to demonstrate what is clear from the treatment of due diligence obligations by the ICJ and numerous areas of activities where only soft-law obligations exist, that assertions of due diligence being a universal standalone source from which it is possible to automatically identify binding obligations for any area of activities is incorrect as a matter of law, and it is for States to decide whether to establish primary rules containing due diligence obligations in relation to the attributes of those specific contexts.

This conclusion does not preclude binding obligations from developing in the future should sufficient State practice and *opinio juris* emerge for a rule containing such obligations in cyberspace to crystallize. Indeed, the statements by an increasing number of States encouraging or endorsing binding due diligence obligations in relation to cyber operations may indicate the early stages of such a process. This would be in line with consensus UN GGE reports which explicitly recognize that challenges presented by the 'unique attributes' of cyber operations means 'additional norms could be

developed over time',[232] and that 'existing norms may be formulated for application to the ICT environment … where additional norms that take into account the complexity and unique attributes of ICTs may need to be developed'.[233] Similarly, the final report of the UN OEWG, also adopted by consensus, recognized that 'additional norms could continue to be developed over time'.[234] The ICJ may also play an important role in the development of custom through the method of assertion in recognizing rules as being of customary status.[235] Another attempt to bypass insufficient State practice and *opinio juris* for a customary rule containing due diligence obligations in cyberspace is by claiming there exists a general principle of due diligence in the sense of Article 38(1)(c) of the ICJ Statute.[236] However, this assertion is particularly difficult to maintain given the controversial nature of the existence of a category of 'general principles of law formed within the international legal system'[237] in addition to the contrary treatment of such obligations in ICJ case law outlined in this article.

Nonetheless, the role of scholarship that has sought to misrepresent *lex ferenda* as *lex lata* in encouraging such a development should be understood as remarkable for the reasons outlined in this article. If assertions that due diligence is a universal standalone source from which it is possible to derive binding obligations for all areas of activity as promoted in academic projects as a basis to identify binding obligations in cyberspace receives widespread acceptance from States, this would constitute a radical transformation of the international rules-based system, broadening obligations of conduct for States in an unprecedented manner beyond the cyber context. Not only are assertions of binding due diligence obligations in cyberspace resulting from a supposed universal standalone source of due diligence as *lex lata* disingenuous in that they contradict the case law of the ICJ and lack supporting legal authority outside of cyber-specific literature, but they also contradict the position of States in UN fora and State practice in cyberspace. Moreover, their presentation as such serves to misrepresent and distort dangerously the status of fundamental legal principles, rules and obligations of conduct in international law, and undermine any stability and support that they provide

[232] 2013 GGE Report (n 1) 8; 2015 GGE Report (n 1) 7; 2021 GGE Report (n 1) 8.

[233] 2015 GGE Report (n 1) 7; also see the 2010 GGE Report (n 147) 8, which notes that '[g]iven the unique attributes of ICTs, additional norms could be developed over time'.

[234] OEWG Final Report (n 3) 5.

[235] See S Talmon, 'Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion' (2015) 26 EJIL 417. Some authors have challenged certain assertions of the Court where *opinio juris* did not appear to be present. See Tams, who argues that 'anything goes in the ascertainment of custom', in C Tams, 'Meta-Custom and the Court: A Study in Judicial Law-Making' (2015) 14 LPICT 51, 79; and Benvenisti, who considers that 'the ICJ or other tribunals "cheat" by inventing what they refer to as custom', E Benvenisti, 'Customary International Law as a Judicial Tool for Promoting Efficiency' in E Benvenisti and M Hirsch (eds), *The Impact of International Law on International Cooperation: Theoretical Perspectives* (CUP 2004) 87.

[236] Schmitt (n 8) 31.

[237] See Wood (n 116); Vázquez-Bermúdez and Crosato (n 116) 168–71; Pomson (n 116).

outside of the cyber context. As d'Aspremont notes, 'legal scholars have continuously found in the theory of customary international law a convenient instrument to vindicate the progressive development of international law and its expansion in areas which they perceive as being insufficiently regulated by it'.[238] Such claims, carefully crafted to avoid the obstacles of insufficient State practice and *opinio juris*, are best understood as a form of interventionism, that is, an attempt to intervene in the problems of the world by stretching existing legal frameworks to address what they perceive to be dangerous legal gaps,[239] openly seeking to provide States with recourse to countermeasures in spite of the contrary position of the ICJ and States on the existence of such rules. Perhaps such concerns over the interventionist role of scholars informed the unfortunate veto by States to block further engagement of groups including the Oxford Institute for Ethics, Law and Armed Conflict in the UN OEWG.[240]

ACKNOWLEDGEMENTS

The author would like to thank Professor Catherine Redgwell (University of Oxford) and Dr Efthymios Papastavridis (University of Oxford) for their comments and suggestions on the doctoral thesis chapter on which this article was based.

[238] J d'Aspremont, 'Customary International Law as a Dance Floor: Part I' (*EJIL Talk!*, 14 April 2014) <https://www.ejiltalk.org/customary-international-law-as-a-dance-floor-part-i/>.

[239] See J d'Aspremont, 'Cyber Operations and International Law: An Interventionist Legal Thought' (2016) 21 JC&SL 575; see recent comments of Akande (Oxford Institute for Ethics, Law and Armed Conflict) in support of such assertions that refer to 'dangerous gaps in international law framework applicable to cyber operations', P Berman et al, 'Panel 12: Cyberwarfare and Other Challenges to the Law of Armed Conflict' (The London Conference on International Law 2022, Queen Elizabeth II Centre, London, 11 October 2022) <https://vimeo.com/760397545>.

[240] See Cybersecurity Tech Accord, 'Industry Perspective Rejected: Cybersecurity Tech Accord Releases Joint Statement on Veto by UN Cyber Working Group' (*Cybersecurity Tech Accord*, 21 July 2022) <https://cybertechaccord.org/industry-perspective-rejected-cybersecurity-tech-accord-regrets-decision-by-states-to-reject-participation-in-un-open-ended-working-group-on-cybersecurity/>.