The Attribution of Omissions: Due Diligence in Cyberspace and State Responsibility

Evelyne Schmid & Ayşe Özge Erceiş*

Cyber operations can cause significant disruption. When a state fails to do what is arguably required to prevent, halt, mitigate or repress cyber operations, the nature of the relevant conduct is a potential failure to exercise due diligence, in other words, an omission. Illustrated with a case study on cyberspace, we aim to show that the attribution of omissions in the international law of state responsibility is far more straightforward than what states seem aware of. We conduct a comparative analysis of a set of reports submitted by states about how international law applies in cyberspace to examine how states deal with the attribution issues around failures to exercise due diligence. After more than twenty years of existence, the ILC Articles on State Responsibility are the uncontroversial reference point for the analysis of state responsibility and examining them in relation to omissions underscores their practicality in addressing due diligence failures.

Keywords: Cyberspace – state responsibility – attribution – omissions – due diligence

Table of Contents

I. Introduction: The Research Question and Why It Matters
II. The Raw Material: States' Published Positions on International Law in Cyberspace, Why and How We Examined Them
III. The Attribution of Failures to Act in the ILC Articles on State Responsibility: The Law
IV. State Positions on the Attribution of Due Diligence Failures: What States Make of the Law so Far
V. The Way Forward and Concluding Thoughts

I. Introduction: The Research Question and Why It Matters

In this article, we report about how states discuss attribution questions for failures to exercise due diligence in relation to malicious cyber operations. International law today requires states to take various policy measures to prevent harm from non-state actors, to mitigate risks and to protect populations from dangers, such as from cyber

* Evelyne Schmid is a professor of international law at the University of Lausanne (evelyne.schmid@unil.ch). Ayşe Özge Erceiş is a PhD Candidate in public international law at Paris Panthéon Assas University working on state responsibility in cyberspace. The first author thanks the Swiss Ministry of Foreign Affairs for the invitation to contribute to an expert dialogue on how international law applies in cyberspace in fall 2021 and a subsequent discussion at the Swiss Ministry of Foreign Affairs in November 2021. This text is written solely in the authors' personal capacity.

operations, environmental harms, domestic violence, or harm to foreign investors, to name just a few. States must adopt their legislative frameworks, set up infrastructures, train and make available staff and take a plethora of other measures to comply with their positive obligations stemming from various branches of international law, such as human rights law, environmental law, international economic law or security and disarmament law. Such due diligence obligations have become a topic of growing interest in relation to cyber matters as cyber threats have evolved dramatically. The 2000s saw cyber activities shift from sporadic events to orchestrated attacks, highlighted by the Estonia Cyberattacks in 2007 and Operation *Aurora* in 2009 against Google and other companies. In the following decade, this trend amplified. Notable incidents like the *Stuxnet* worm in 2010, the 2014 *Sony Pictures* hack, and widespread malware attacks in 2017, such as *WannaCry* and *NotPetya,* emphasise the increasing entanglement of cyber operations with international politics.

When states fail to take the necessary measures, the attribution of failures to exercise due diligence is a key issue in the international law of state responsibility. State responsibility and due diligence have evolved significantly in international law. Historically rooted in diplomatic protection, the idea of due diligence broadened from addressing harm to a state's nationals to the protection of many other interests of states but also individuals, international organisations, or the environment.

Importantly, due diligence is not a single norm, but a plurality of norms.[1] Due diligence can be a legal standard that is qualifying other norms, such as positive human rights obligations, or it can be a stand-alone norm referring to the famous idea stated by the International Court of Justice in the Corfu Channel Case (1949) that each state must «not to allow knowingly its territory to be used for acts contrary to the rights of other states».[2] Attribution refers to the exercise, in international law, to connect conduct with a state.[3] We use the term «attribution» in the narrow sense, as described by Gábor Kajtár as «exclusively a state responsibility concept, which serves for imputing internationally wrongful acts to states»,[4] because we are exclusively interested in this article in how states conceive state responsibility for due diligence failures in cyber matters. We focus on cyber operations and state responsibility because states have recently spent considerable time and effort to conceptualise the attribution issues in this field (section II). We conduct a comparative analysis of a set

1 Antonio Coco & Talita de Souza Dias, «‹Cyber Due Diligence›: A Patchwork of Protective Obligations in International Law», 32 European Journal of International Law (2021), 771–805, at 782.

2 *Corfu Channel Case* (United Kingdom v Albania) [1949] ICJ Rep 4 at 22.

3 James Crawford, State Responsibility. The General Part, Cambridge 2013, at 113, referring to the «process by which international law establishes whether the conduct of a natural person or other such intermediary can be considered an 'act of state' and thus give rise to state responsibility».

4 Gábor Kajtár, «Fragmentation of Attribution in International Law», in: G. Kajtár et al. (eds), Secondary Rules of Primary Importance in International Law: Attribution, Causality, Evidence, and Standards of Review in the Practice of International Courts and Tribunals, Oxford 2022, 283–301, at 284.

of position papers submitted by states about how international law applies in cyberspace,[5] and we find that there is a disconnect between the analysis of due diligence and the question of attribution for the purposes of the law of state responsibility for internationally wrongful acts. Our key premise is that when a state fails to exercise due diligence, the nature of the relevant conduct is a failure to act, i.e. an omission and we observe that states do not seem entirely clear about how a failure to exercise due diligence is to be attributed in the existing law of state responsibility.

The starting point for this contribution is that states have shown considerable interest in due diligence in relation to cyberspace. Due diligence is an attractive concept when a cyber operation cannot be attributed to another state.[6] This is because due diligence places the emphasis on the measures a state should (arguably) have taken or take to prevent,[7] mitigate, or halt a cyber operation and minimise its adverse consequences.[8] This interest in due diligence in relation to cybersecurity thus stems from the fact that a victim state can try to argue that another state failed to take sufficient measures and the invoked international law violation is not the cyber operation but the lack of measures.[9] The Tallinn Manual 2.0 acknowledges that the term «act» for the purposes of state responsibility «refers to both actions and omis-

5 Whenever we refer to the term «cyberspace», we do not refer to a new legal domain, nor a new type of «space» (in addition to land, sea, air and space). We simply refer the term as a shorthand for «the Internet together with other computers and telecommunications networks». François Delerue, Cyber Operations and International Law, Cambridge 2020, at 9 et seq., 12. For more elaboration about the term (in German), see Lorez Langer, «Cyberspace Does Not Lie within Your Borders: Jurisdiktion und Menschenrechte im Digitalen Raum», 29 Swiss Rev. Int'l & Eur. L. (2019), 3–21, at 7 et seqq.

6 See, for instance, the reports of Japan or the Netherlands in the «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», A/76/136, 13 July 2021, Japan Report p. 49; The Netherlands Report p. 5.

7 The preventive component of due diligence is controversial (as is generally prevention in the law of state responsbility), see Sarah Cassella, «Les travaux de la Commission du droit international sur la responsabilité internationale et le standard de due diligence», in: S. Cassella (ed.), Le standard de due diligence et la responsabilité internationale: Journée d'études du Mans, Paris 2018, 11-24, at 15-16. But there are due diligence obligations within specific sub-branches of international law, such as human rights law where due diligence is a qualifying standard to interpret treaty obligations. Many of these clearly have preventive dimensions (such as the obligation to take steps to prevent the deterioration of health-care facilities and services) and we, therefore, include the preventive dimension in this article. On the controversial aspects of whether due diligence in general (or what the Tallinn Manual 2.0 calls «the due diligence principle») includes a preventive dimension, see Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2 ed., Cambridge 2017, at 44 et seq.

8 About the attractiveness of the due diligence concept, see notably the International Law Association report on Due Diligence, Duncan French et al., «Second Report». (2016), <www.ila-hq.org/en/documents/draft-study-group-report-johannesburg-2016> (last accessed on 9 May 2023).

9 Samantha Besson, La due diligence en droit international, La Haye 2021, at 262.

sions»,[10] and emphasises that care must be taken «to distinguish application of the due diligence principle from the international wrongfulness of the particular cyber operation that has been mounted from, or employed cyber infrastructure on, the State's territory»,[11] thus suggesting that we do not worry about the attribution of a cyber operation to a state in case of failures to exercise due diligence, but rather the lack of measures taken by the state. The Tallinn Manual 2.0, developed by experts and commissioned by NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), is an influential study applying international law to cyberspace, offering 154 rules and commentary related to international law and cyber operations. The Tallinn Manual 2.0 explicitly notes that «[t]he due diligence principle is a legal obligation that is violated by omission. In this regard, omission not only encompasses inaction, but also the taking of ineffective or insufficient measures when other more appropriate measures are feasible, that is, reasonably available and practicable.»[12] The Tallinn Manual 2.0 thus confirms the interest in due diligence in cyberspace.

Before diving into attribution, we need to establish why we will treat due diligence obligations as primary obligations. The vast majority of obligations in international law are so-called primary obligations, i.e. all obligations states have incurred in treaties, customary law and other sources and which contain substantive and procedural obligations that states must comply with. Secondary rules are only those that deal with the consequences of a violation of a primary rules, such as the rules used to establish attribution, circumstances excluding wrongfulness or reparations. The work of the ILC to codify the international law of state responsibility has aimed to confine due diligence to primary obligations,[13] and this is how we will proceed in this contribution. This treatment of due diligence is justified given the development and multiplication of positive obligations of conduct means today that there are numerous ways in which states can fail these positive obligations, including in relation to relatively new fields such as cybersecurity.[14] This background implies that there is today sufficient material to analyse questions of how failures to comply with such obligations of conduct can lead to state responsibility. Obligations of conduct require states to «take all measures reasonably available to it in order to prevent harm from occurring».[15] In relation to cyberspace, due diligence obligations can entail that states must analyse cyber risks, collaborate with other states to mitigate risks and

10 Tallinn Manual 2.0, supra n. 7, at 80.

11 Tallinn Manual 2.0, supra n. 7, at 42.

12 Tallinn Manual 2.0, supra n. 7, at 43.

13 Besson, supra n. 9, at 61.

14 Even if this debate is beyond the scope of the present article, it is warranted to mention that Samantha Besson also notes how due diligence is possible to exist as a legal concept even in the absence of a positive obligation: Besson, supra n. 9, at 83 et seq.

15 Vladyslav Lanovoy, «Causation in the Law of State Responsibility», British Yearbook of International Law (2022), at 22.

exchange vital intelligence. Because these are obligations of conduct, if a state can show that it has taken the necessary measures required by a due diligence obligation, it will not incur responsibility even if harm occurs. This analysis of due diligence obligation is exclusively situated at the level of the analysis of the breach, i.e., the primary obligation.

Yet, some have legitimately questioned whether due diligence is a concept that is entirely part of primary obligations.[16] Due diligence is closely linked to negligence and the idea that states as abstract entities can be negligent raises the old question of whether state responsibility should have «subjective» or «moral» aspects. Although some remains of subjectivity in state responsibility linger,[17] the ILC has answered in the negative – stating that state responsibility is an objective standard and fault, or negligence are only relevant if the primary obligation contains such subjective elements. In this view, due diligence is part of primary obligations – either as a specific obligation by and of itself (such as, e.g. general due diligence obligations relevant in relation to cyber security, such as the obligation not to allow one's territory to be used to harm the functioning of another state's authorities), or as a standard qualifying another obligation (such as an obligation of the state to protect human rights against harm). Even if it is the «primary obligations type of due diligence» that we focus on in this article, it is warranted to at least flag the complex debate to readers. Besson recounts how each tentative to neatly conceptualize due diligence as either only primary or only secondary obligations has failed throughout the 20th century.[18] In line with a recent study of the Oxford Institute for Ethics, Law and Armed Conflict, we suggest that the easiest and most convincing approach is to view due diligence not as a single obligation or concept, but a bundle of obligations,[19] many of which fit squarely within primary obligations, while others, such as the due diligence to avoid state complicity, are difficult to qualify as either primary or secondary obligations. What is important to follow the present contribution is that states are interested in due diligence in relation to cybersecurity, and that we limit ourselves to due diligence obligations at the level of primary obligations.

Despite states' interest in due diligence failures in cyberspace and state responsibility, at least some states seem uncertain about how to connect the two. Some states present due diligence as some sort of an alternative framework outside the Interna-

16 For an excellent summary of the debate Helmut Philipp Aust & Prisca Feihle, «Due Diligence in the History of the Codification of the Law of State Responsibility», in: H. Krieger et al. (eds), Due Diligence in the International Legal Order, Oxford 2020, 42–58, at 42 et seqq.

17 Such as in relation to complicity, see ibid., at 54.

18 Besson, supra n. 9, at 53.

19 Talita de Souza Dias & Antonio Coco, «Cyber Due Diligence in International Law», Oxford Institute for Ethics, Law and Armed Conflict, Blavatnik School of Government, Oxford 2021, at. 15; Coco & de Souza Dias, «‹Cyber Due Diligence›: A Patchwork of Protective Obligations in International Law», 32 European Journal of International Law (2021), 771–806.

tional Law Commission's Articles on State Responsibility for Internationally Wrongful Acts (ILC Articles or ARSIWA) for situations in which state responsibility would, in their view, otherwise be impossible to establish. We find this view idiosyncratic and unconvincing. By analysing various state positions in relation to international law in cyberspace, we diagnose that the authors of a number of state reports are unnecessarily unclear or confusing about the attribution of omissions. Our main finding in this article is that the attribution of omissions is squarely possible in the law of state responsibility, although this possibility is weakly acknowledged in current debates on international law in cyberspace, which tend to focus on how a cyber operation itself can be attributed to a foreign state, while glossing over or at times misrepresenting the attribution of failures to exercise due diligence.

Achieving clarity on the question of attribution of omissions is significant for three reasons. First, from a practical point of view, even where a state has reason to suspect another state to be behind a cyber operation, gathering the necessary evidence is often elusive and the attention thus turns to a failure to exercise due diligence.[20] In practice, attributing conduct to a state is a complex national political decision based on technical and legal considerations regarding a specific cyber incident or operation.[21] Attributing cyber operations can be difficult or impossible for a variety of reasons, such as the fact that cyber risks and sources of harm are diverse, cyber operations are often technically complex, sometimes of a collective nature e.g. with a large number of individual perpetrators involved, and actors who conceal their identities and operate secretly. Malicious cyber-operations usually entail using stand-ins or actors formally independent of the state to execute the actual cyber offensive, thereby making legal attribution linking the operation to the sponsoring state sponsoring daunting. Consider, for instance, the *Stuxnet* attack[22] that had Iran's nuclear program in its crosshairs and is widely considered to be the result of a collaboration between the United States and Israel, but uncertainties remain.[23] The complexity of the worm discovered in 2010 and the use of stand-ins to execute the operation meant that attributing the operation to those states in an accurate and timely manner was speculative. In another well-known example, the *WannaCry* ransomware attack, legal attribution of the cyber operation as such to a state was similarly difficult, with suspected North Korea denying the allegations: the *WannaCry* ransomware attack

20 Kubo Mačák, «Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors», 21 Journal of Conflict and Security Law (2016), 405–428, at 428.

21 Nicholas Tsagourias & Michael Farrell, «Cyber Attribution: Technical and Legal Approaches and Challenges», 32 European Journal of International Law (2020), 941–967, at 942.

22 Andrew C. Foltz, «Stuxnet, Schmitt Analysis, and the Cyber Use-of-Force Debate», 67 Joint Force Quarterly (2012), 40–48, at 41.

23 Marie Baezner & Patrice Robin, «Hotspot Analysis: Stuxnet», Center for Security Studies, ETH Zurich (2017), <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf> (last accessed on 22 August 2023).

caused widespread disruption globally, impacting hundreds of thousands of computers in over 150 countries, including computers of health-care facilities. A non-state actor, the Lazarus group thought to consist of North Korean and Chinese individuals, might also have been involved, leading to ambiguity.[24]

When the information available is insufficient to ascertain with sufficient certainty that a cyber operation can, in one way or another, be attributed to another state, the victim state still has the option to analyse whether another state has failed its due diligence obligations. A victim state can often ascertain more easily that another state failed to exercise due diligence when we do not know, or cannot prove, where the cyber operation took its origin and attribution of the actual cyber operation e.g. by way of article 8 ARSIWA is unrealistic, be it because the control test of article 8 ARSIWA is too challenging or simply because the information is not available.[25] For instance, the cyber operations on Estonia, Georgia, Ukraine or the allegations regarding cyber interferences in elections all raise questions of at least a failure of due diligence on the part of Russia to prevent its territory from being used for malicious cyber operations, whereas technical details and certainty about the precise involvement of the state in the actual operations remain contested or unclear.[26] In conclusion, while it may often be challenging to link actual cyber engagements to states, there have been multiple instances where the available information at least indicates that a state did not take sufficient reasonable steps to prevent, halt or mitigate malicious cyber conduct on its territory.

Second, a clear view on the basis for attribution and the nature of conduct that is attributable in cases of cyber operations by private or unknown actors frees up time and energy for a debate about the substantive obligations of states in the field of cyberspace, namely the scope of due diligence obligations. Although states have made some progress in clarifying mutual normative expectations in relation to the substance of due diligence, much work remains to be done.[27] At least eight out of the eleven «UN norms of responsible behaviour in cyberspace»[28] are primarily positive obligations, i.e. obligations to act, such as by taking steps to prevent the misuse of information and communications technologies in the state's territory, cooperate

24 Eric Talmadge & AP News, «Experts question North Korea role in WannaCry cyberattack, 19 May 2017», <https://apnews.com/general-news-ed3298eaaff84e8ebb091cbbd4bc4ab6> (last accessed on 9 August 2023).

25 About the difficulties with the applicable control test for attribution of cyber conduct by way of Article 8 ARSIWA, see notably Mačák, supra n. 20, at 408 et seqq.; Yannick Zerbe, «Cyber-Enabled International State-Sponsored Disinformation Operations and the Role of International Law», 33 Swiss. Rev. Int'l & Eur. L. (2023), 50–76, at 60.

26 Sean Cordey, Cyber Influence Operations: An Overview and Comparative Analysis, Zurich 2019, at 20, 22.

27 Coco & De Souza Dias, supra n. 19, at 771.

28 Australian Strategic Policy Institute, UN Cyber Norms, <www.aspi.org.au/cybernorms> (last accessed on 6 July 2023).

with other states, protect critical infrastructure and report vulnerabilities. These «eleven UN cyber norms» are a set of norms «setting out what states should and should not do in the digital space».[29] States insist that they are «voluntary», although at least some of them are most probably authoritative interpretations of existing due diligence obligations or part of customary law. We do not need to clarify the precise legal nature of the different norms here. Suffice it to say that the «eleven UN cyber norms» confirm that states themselves underline the importance of state measures to prevent, monitor, report, cooperate and regulate – in other words to exercise due diligence. As in other fields, states have long accepted that their mere abstention is not good enough – not instructing or allowing their state organs to conduct a cyber operation is not sufficient. In light of this widespread acceptance of positive obligations, it seems useful if we could at least already clarify the attribution of failures to comply with such positive obligations because such clarity places states in a better position – if they so wish – to meaningfully discuss the due diligence obligations and the implications for states who breach them.

Third, and beyond the debate on international law in cyberspace, the current conceptual confusion on attribution for failures to exercise due diligence obscures the potential and usefulness of the ILC Articles and risks diminishing the status of due diligence norms in existing positive law. The ILC Articles have become a key reference in international legal practice.[30] They also deserve to be taken seriously when it comes to the attribution of omissions, i.e. failures to exercise due diligence. We aim to show that ARSIWA are far more straightforward than what states seem aware of when it comes to cyber operations by private (or simply unknown) actors. The significance of this finding goes beyond the debates on international law in cyberspace and also appears in other fields such as environmental law or human rights law, including in some of the high-profile climate litigations. We hope that our analysis of how alleged failures to exercise due diligence in relation to cyber operations will contribute to clarify how attribution for the purposes of state responsibility works for claims of insufficient state action more generally.[31]

29 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, A/AC.290/2021/CRP.2, paras 7 and 8.

30 Federica Paddeu & Christian Tams, «Dithering, Trickling Down, and Encoding: Concluding Thoughts on the ‹ILC Articles at 20› Symposium», European Society of International Law (2021), <www.ejiltalk.org/dithering-trickling-down-and-encoding-concluding-thoughts-on-the-ilc-articles-at-20-symposium/> (last accessed on 7 July 2023).

31 Such as in the Swiss climate case of the Swiss Elderly Women (Klimaseniorinnen) pending before the European Court of Human Rights, where the alleged violations mostly concern allegations of failures to take sufficient measures. Evelyne Schmid, «Victim Status before the ECtHR in Cases of Alleged Omissions: The Swiss Climate Case», (2022), <www.ejiltalk.org/victim-status-before-the-ecthr-in-cases-of-alleged-omissions-the-swiss-climate-case/> (last accessed on 9 August 2023).

We structured this article in the following way: In section II, we situate the debate on legal attribution in relation to cyber operations and we explain what material we analysed and how. In section III, we outline how the ARSIWA deal with the attribution of failures to exercise due diligence and why this framework is relevant and, in our view, perfectly suitable in relation to international law in cyberspace. The core of our analysis is in section IV, where we present the comparative examination of states' position papers. We look at whether and how states conceptualize attribution of failures to exercise due diligence. We identify a number of surprising presentations of attribution issues and the erroneous idea that due diligence failures exist outside the accepted framework of attribution in the law of state responsibility. We use section V to conclude with reflections about this – in our view – unfortunate situation. We suggest that the preferred course of action entails that states pay increasing attention to the fact that the attribution of omissions in the law of state responsibility is already foreseen in current international law and the real locus of debate is the scope of the due diligence obligations, but not the attribution of failures to exercise such diligence.

In order to set the stage for explaining our suggestion, we now briefly turn to the context in which numerous states positioned themselves on matters of international law in relation to cyber operations and we explain what material we included in our analysis and why this material is of particular interest for an analysis of attribution issues for failures to act.

II. The Raw Material: States' Published Positions on International Law in Cyberspace, Why and How We Examined Them

Our main source of information is a Compendium of state positions. This Compendium emerged in the context of the United Nations Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266 (A/76/136).[32] A total of fifteen states collaborated on the Compendium, spanning different geographical regions and economic profiles: Australia, Brazil, Estonia, Germany, Japan, Kazakhstan, Kenya, the Netherlands, Norway, Romania, the Russian Federation, Singapore, Switzerland, the United Kingdom of Great Britain and Northern Ireland, and the United States of America.

The Compendium has 142 pages and includes translations of some of the reports into several United Nations official languages, highlighting its international significance and accessibility. The Compendium contains voluntary national contributions

32 Official Compendium, supra n. 6.

on the subject of how international law applies to the use of information and communications technologies by states and we will refer to «the Compendium» in what follows.

The UN GGE aimed to ensure that states adopt responsible behaviour by not knowingly allowing their territory to be used for internationally wrongful acts using Information and Communication Technologies (ICTs).[33] Alongside this UN GGE, an Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) published its final report in 2021,[34] also with a compendium of state statements in explanation of position on the final report (25 March 2021).[35] This second compendium is, however, merely a collection of statements explaining the reasons why, or to what extent, states supported the OEWG final report. These explanations are of complementary indication that most states generally affirm the relevance of existing international law in relation to cyber activities. That said, the UN GGE Compendium reveals far more about individual states' positions on legal attribution in relation to cyber matters than the OEWG documents, which is why we focus on the GGE Compendium.

Recently, a broad coalition of almost 50 states put forward a resolution at the UN General Assembly First Committee welcoming the proposal to establish a United Nations programme of action to advance responsible State behaviour.[36] In November 2020, UN member states also established, through Resolution A/C.1/75/L.8/Rev.1 a second OEWG; this time expected report back to the General Assembly in 2025.[37] The fact that there are two concurrent UN processes to study, the GGE and the OEWG – each with advantages and disadvantages – was due to disagreements amongst states on key legal and institutional questions and geopolitical tensions.[38] Be

33 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013, <https://digitallibrary.un.org/record/753055> (last accessed on 26 April 2023), at 23; Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 24 July 2015, at 13(c).

34 Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Report, A/AC.290/2021/CRP.2, 10 March 2021.

35 Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Compendium of Statements in Explanation of Position on the Final Report, A/AC.290/2021/INF/2, 25 March 2021.

36 United Nations, General Assembly, Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security, A/C.1/77/L.73, 13 October 2022.

37 United Nations, General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, A/C.1/75/L.8/Rev.1, 26 October 2020.

38 Daniel Stauffacher, «UN GGE and UN OEWG: How to Live With Two Concurrent UN Cybersecurity Processes, Remarks at the Jeju Forum May 2019», ICT4Peace. (2019), <https://ict4peace.org/publications/un-gge-and-un-oewg-how-to-live-with-two-concurrent-un-cybersecurity-processes/> (last accessed on 22 May 2023).

this as it may, both processes documented widespread agreement of UN members, at least at the surface, that international law applies to cyberspace. In short, the 2021 UN GGE Compendium is by far the most instructive document for our purposes. It contains the most recent and detailed documents produced by states, the reports are easily accessible and provide the most comprehensive documentation of how at least this group of states view the attribution issues for failures to exercise due diligence in cyberspace. It is clear that this dataset has limitations. By far not all states were part of the UN GGE exercise and from those who are, not all states express a view on attribution in their voluntary contribution. Moreover, the Compendium contains the included states' views on a wide range of other issues related to international law questions and cyberspace: we only focus on two of them and the relationship between them: attribution and due diligence. As a complementary resource, we recommend to readers the interactive «Cyber Law Toolkit» prepared by Dr Kubo Mačák and his team. This toolkit is an online resource which collects published state positions on international law in cyberspace as well as numerous hypothetical scenarios of cyber operations, each with a suggested legal analysis.[39] Most recently, Costa Rica,[40] Denmark,[41] Ireland,[42] and Pakistan[43] published national position papers in 2023, underlining the sustained interest states show in this topic although their positions are not included in the Compendium. Despite these limitations the Compendium allows us to make a few conceptual points. We examine how each state report mentions the articles on attribution in the law of state responsibility (arts. 4–11 ARSIWA), whether the analysis of attribution is linked with due diligence and if so, how.

For what we intend to show in this article, we now need to briefly revisit the ARSIWA and explain how the ILC Articles deal with omissions.

39 NATO Cooperative Cyber Defence Centre of Excellence, The Cyber Law Toolkit, <https://cyberlaw.ccdcoe.org/> (last accessed 6 July 2023).

40 Ministry of Foreign Affairs of Costa Rica, «Costa Rica's Position on the Application of International Law in Cyberspace», 21 July 2023, <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf> (last accessed on 22 August 2023).

41 Jeppe Mejer Kjelgaard & Ulf Melgaard, «Denmark's Position Paper on the Application of International Law in Cyberspace: Introduction», 92 Nordic Journal of International Law (2023), 1–10.

42 Irish Department of Foreign Affairs, «Position Paper on the Application of International Law in Cyberspace», 6 July 2023, <www.dfa.ie/media/dfa/ourrolepolicies/internationallaw/Ireland---National-Position-Paper.pdf> (last accessed on 22 August 2023).

43 The Permanent Mission of Pakistan to the United Nations, «Pakistan's Position on the Application of International Law in Cyberspace», 3 March 2023, <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNODA.pdf> (last accessed on 22 August 2023).

III. The Attribution of Failures to Act in the ILC Articles on State Responsibility: The Law

Not exercising due diligence equates to a state's omission, failing to meet its positive obligation. Although, in English, they are called the Articles on Responsibility of States for Internationally Wrongful *Acts,* Article 2 of ARSIWA confirms that an internationally wrongful «act» of a state can be conduct «consisting of an action or omission».[44] As the Commentary to Art. 1 ARSIWA further emphasizes: «An internationally wrongful act of a State may consist in one or more actions or omissions or a combination of both.»[45] The French term «fait internationalement illicite» or the Spanish «hecho internacionalmente ilícito» more aptly capture the idea that wrongfulness can result from omissions as well as from acts.[46] The International Law Commission regretfully notes in its Commentary that the English language is unable to accurately translate the French or Spanish terms, and that, therefore, the term «wrongful act» was the term retained in the English version but that it was clear that «the term ‹act› is intended to encompass omissions, and this is made clear in article 2».[47]

If omissions are clearly covered in the law of state responsibility, how are they to be attributed to a state? The usual rules of attribution apply. Pierre d'Argent and Alexia de Vaucleroy state that attribution of omissions is even a no-brainer and only requires us to identify that the state was required to act but failed to do so.[48] According to them, we do not have to specify which rule of attribution is at stake and the only issue is the scope of the obligation invoked and whether the state took sufficient measures to comply with it: «attribuer une omission à un sujet ne requiert pas de déployer les règles d'attribution bien connues du droit de la responsabilité internationale, mais seulement d'identifier le sujet débiteur de l'obligation positive [et] la difficulté réside ainsi dans la détermination du contenu de l'omission illicite.»[49] In response to that view, Samantha Besson criticizes d'Argent and de Vaucleroy and argues that the two authors too quickly associate the question on the scope of the obligation with attribution.[50] Besson's disagreement stems from the fact that d'Argent and de Vaucleroy state that it is enough to identify that the state should have taken measures and failed to do so, rather than separating the attribution analysis from the

44 ILC Articles on State Responsibility, Annex to GA Res. 56/83, 12 December 2001, Art. 2.

45 Ibid., Commentary to Art. 1, para. 1.

46 Ibid., Commentary to Art. 1, para. 8.

47 Ibid.

48 Pierre d'Argent & Alexia de Vaucleroy, «Le contenu de l'omission illicite : la non utilisation de moyens raisonnables», in: S. Cassella (ed.), Le standard de due diligence et la responsabilité internationale: Journée d'études du Mans, Paris 2018, 255–278, at 260.

49 Ibid.

50 Besson, supra n. 9, at 204, footnote 492.

analysis of the breach. Yet, each one has a point. D'Argent and de Vaucleroy invite us to consider the ease at which attribution is legally possible for omissions in breach of a primary obligation. The omission is necessarily the state's own conduct. The Permanent Court of International Justice famously said that «[s]tates can act only by and through their agents and representatives»,[51] and states can also fail to act only by and through their agents and representatives, and the ARSIWA allow us to decide what constitutes an organ or otherwise an agent of a state for purposes of responsibility.[52] In our view, d'Argent and de Vaucleroy are not oversimplifying by stating that the focus of the analysis will shift to the question of whether the state has failed to comply with a positive obligation and thus the question whether there is a breach. The two authors are correct to highlight the fact that as soon as we know that a state had a due diligence obligation, the lack of the required measures is necessarily an omission of that state's organs.

Nevertheless, Besson's point not to merge the analysis of the breach with the one of attribution is well-placed and helpful. There is no need to skip the analysis of the traditional attribution rules. Rather, attribution always occurs by way of article 4 of the ILC Articles. In other words, it is easy to attribute omissions because the answer is always article 4 of the ILC Articles. As Franck Latty points out, «the operation of the rules of attribution of conduct in relation to omission operates at a greater level of abstraction», but they remain the same.[53] This idea is also recognized in the Commentary of the ILC. The ILC speaks of finding a state responsible for a failure «to take necessary measures to prevent» effects of private parties and states that in such constellations, «there is often a close link between the basis of attribution and the particular obligation said to have been breached, even though the two elements are analytically distinct».[54] In sum, the attribution rules remain unchanged and are straightforward for failures to exercise due diligence whereas the determination of the scope of the due diligence obligation is unfortunately not.

If attributing failures to exercise due diligence obligations does not raise complex difficulties, one could end the analysis here. Yet, our survey of the Compendium of state positions reveals that the elegancy of the ILC Articles in relation to the attribution of omissions is underexplored. In the next step, we show what states say about the link between the rules of attribution and due diligence in cyberspace.

51 Questions Relating to Settlers of German Origin in Poland (Advisory Opinion of 10 September 1923) 1923 PCIJ Series B no. 6, at 22.

52 ILC Articles on State Responsibility Commentary, at 39.

53 Franck Latty, «Actions and Omissions», in: J. Crawford et al. (eds), The Law of International Responsibility, Oxford 2010, 355–369, at 360–361. See also Sarah 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 & S. Heathcote (eds), ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case, London 2012, 295–314, at 310.

54 ILC Articles on State Responsibility Commentary, at 39.

IV. State Positions on the Attribution of Due Diligence Failures: What States Make of the Law so Far

This section examines how states reference ILC Articles rules on attribution in their reports and their stance on attributing failures in exercising due diligence. We proceeded in three steps.

In a first step, we considered whether states acknowledge the possibility of state responsibility for failures to act and whether they base the analysis on the ILC Articles. We found that nine out of the 15 states represented in the Compendium indeed explicitly refer to omissions in their reports and refer to the ILC Articles when they mention omissions: This is the case for Australia,[55] Brazil,[56] Estonia,[57] Japan,[58] the Netherlands,[59] Norway,[60] Romania,[61] Switzerland,[62] and the United States of America[63]. Estonia, Norway, and Brazil particularly cite article 2 ARSIWA, whereas the others make broader references to the ARSIWA or simply to the «law on state responsibility». The Russian Federation mentions omissions in relation to state responsibility «governed by international law».[64] Upon initial review, it thus seems that numerous states recognize that there can be responsibility for lack of action and these states believe that the ARSIWA rules of attribution are the relevant starting point.

In a second step, we analysed more closely how states write about the possibility of responsibility for failures to act, i.e. omissions in cyber matters. A closer look at the reports reveals that the terms «omissions» or «failures to act/to take measures» only appear in passing in the sections in which the states analyse questions of state responsibility. The reports overall focus on the question of how *cyber operations* can or are attributed – hence state responsibility for *active* conduct. States thus write about whether and under what circumstances cyber conduct itself is attributable to another state, while they spend much less attention to explore the responsibility for omissions. A few examples, in alphabetical order, shall serve to illustrate this tendency: Brazil, as mentioned, affirms that omissions can give rise to state responsibility, reliably cites article 2 ARSIWA for this idea and affirms the relevance of the ARSIWA rules of attribution.[65] In the following sentence in its report, Brazil contin-

55 Official Compendium, supra n. 6, Report by Australia, at 7, 16.
56 Official Compendium, supra n. 6, Report by Brazil, at 21.
57 Official Compendium, supra n. 6, Report by Estonia, at 28.
58 Official Compendium, supra n. 6, Report by Japan, at 47.
59 Official Compendium, supra n. 6, Report by the Netherlands, at 61.
60 Official Compendium, supra n. 6, Report by Norway, at 72, footnote 199.
61 Official Compendium, supra n. 6, Report by Romania, at 78.
62 Official Compendium, supra n. 6, Report by Switzerland, at 99.
63 Official Compendium, supra n. 6, Report by the United States of America, at 141.
64 Official Compendium, supra n. 6, Report by the Russian Federation, at 80.
65 Official Compendium, supra n. 6, Report by Brazil, at 21.

ues to elaborate and states that the ILC Articles imply that, «[b]y analogy, if a cyber operation attributable to a state breaches its international obligations, the state is responsible for this internationally wrongful act».[66] This sentence is entirely correct but limits the analysis to actions, i.e. states engaging in conduct that constitutes a cyber operation attributable to the state. The sentence does not take into account the idea of state responsibility for failing to exercise due diligence. Similarly, Estonia affirms that «[i]n principle, both acts and omissions are attributable to states».[67] Yet, in the same paragraph, Estonia affirms that the purpose of attribution was to allow «establishing if a malicious cyber operation is linked with a state in order to invoke the responsibility of that state».[68] This statement, like the one from Brazil, is accurate but incomplete. The analysis overlooks the omission. We can add two more examples. In a section entitled «key messages», Norway emphasises that a condition for state responsibility «for a cyber operation is that the operation, *or the failure to react against the operation,* constitutes a breach of an international obligation of the State».[69] This sentence is confusing as a «failure to react against the operation» is not the same as a responsibility for a cyber operation as such (but rather a separate responsibility for failure to act). The same seems to occur in the report submitted by the USA, in which the USA affirms responsibility for omissions[70] but limits the implications to say that «*[c]yber activities* [thus: probably active conduct] may therefore constitute internationally wrongful acts under the law of State responsibility if they are inconsistent with an international obligation of the State and are attributable to it»,[71] again suggesting that we consider how the cyber activity at such, rather than the failure to exercise due diligence in cyber matters may be legally relevant for state responsibility. From these examples, we can conclude with certainty that these states agree that there can be omissions attributed to a state for the purposes of state responsibility in cyber matters,[72] but the fact that the reports focus on active conduct at least suggests that responsibility for omissions has probably not yet been given detailed thought of the authors of the state reports in these later sections of the reports.

Thirdly, we scrutinized state statements linking due diligence to attribution. The previous step showed that numerous states adhere to the view that there can be responsibility for omissions, but states then do not explore the conditions of state responsibility for omissions in any detail. In the second step, we searched for the key-

66 Official Compendium, supra n. 6, Report by Brazil, at 21.

67 Official Compendium, supra n. 6, Report by Estonia, at 28.

68 Official Compendium, supra n. 6, Report by Estonia, at 28.

69 Official Compendium, supra n. 6, Report by Norway, at 66 (our emphasis). The Norwegian report later states that for state responsibility *for a cyber operation,* «it is a condition that *the cyber operation* is attributable to the State under international law», with no comparable sentence on the attribution of a potential omission to exercise due diligence. See also at 70, footnote 191.

70 Official Compendium, supra n. 6, Report by the United States of America, at 141.

71 Official Compendium, supra n. 6, Report by the United States of America, at 141 (our emphasis).

72 See also Official Compendium, supra n. 6, Report by Norway, at 71, footnotes 192 and 194.

word «omissions», whether or not the term was linked to due diligence. For the third step, we hypothesized that states maybe went into more detail when they use the term «due diligence», hence, we propose a separate third step to analyse if states relate due diligence with attribution questions for the purpose of state responsibility. This third step was also warranted because a number of states mentioned omissions in passing in a section on «state responsibility» in their reports and the same state report then also contains a separate section on «due diligence».

We observed that states discuss due diligence in cyberspace without addressing attribution concerning state responsibility. References to the Corfu Channel case are particularly popular and appear in the reports of numerous states together with the idea of due diligence, but without discussing attribution.[73] Germany summarizes scenarios of state responsibility in cyber matters and then continues that, «*beyond* the mentioned situations of attribution and aid and assistance, a State may also become liable under international law in connection with another State's or a non-State actor's actions if the first State fails to abide by its obligations stemming from the ‹due diligence› principle».[74] Germany thus separates failures to exercise due diligence from the remainder of the discussion of state responsibility (indicated by the term «*beyond*») which suggests that Germany considers the analysis of the attribution of active conduct as the default legal issue whereas due diligence is presented as a concept «in addition» to the framework of state responsibility.

Estonia explicitly presents due diligence as an alternative basis for attribution: From the examined reports, Estonia makes the most detailed links between due diligence and attribution for the purposes of state responsibility and presents due diligence as a fall-back option seemingly outside the framework of the ILC Articles: Estonia states that due diligence exists for situations in which «state responsibility cannot be established».[75] We find this statement surprising – it was this sentence which motivated us to write this article in order to reflect about the current state of international law when it comes to attributing failures to act. What Estonia means is that state responsibility *for the actual cyber operation* cannot be established. But it would be legally inaccurate to retain that due diligence obligations operate outside the «normal» framework of state responsibility: the difference is solely that we attribute an omission to take measures to prevent, limit or redress a cyber operation,

73 Official Compendium, supra n. 6, Report by Germany, at 33, footnote 33, Report by Japan, at 48, footnote 141, Report by the Netherlands, at 59, footnote 156, Report by Norway, at 71, Report by Romania, at 76, Report by Switzerland, at 91, footnote 235, Report by Brazil, at 21, footnotes 12 and 18.

74 Official Compendium, supra n. 6, Report by Germany, at 40 (our emphasis).

75 Official Compendium, supra n. 6, Report by Estonia, at 26. Estonia writes: «The due diligence obligation derives from the principle of sovereignty. A state has the exclusive right to control activities within its territory. At the same time, this means that it is also obliged to act when its territory is used in a manner that adversely affects the rights of other states. Without this obligation, international law would leave injured states defenceless in the face of malicious cyber activity that emanates from other states' territories. This is particularly relevant when state responsibility cannot be established.»

rather than the operation as such. As we have seen above, the attribution of omissions is as well possible as the attribution of active conduct. The responsibility lies in the lack of measures, rather than the cyber operation itself. Estonia's statement thus obscures that the attribution of omissions is part of the law of state responsibility just as is the attribution of active conduct.

Our third step of the analysis thus confirms that those states that addressed the question find due diligence important and conceive responsibility for failures to exercise such due diligence, but at least so far, the state reports do not properly embed this conclusion into the existing international law on state responsibility.

In the last section, we return to the conclusions of section II which presented how attribution for omissions is conceptualised in the ARSIWA in order to draw the implications for the attribution of failures to exercise due diligence.

V. The Way Forward and Concluding Thoughts

We have defended the view that states could make better use of the ILC Articles to underpin claims of state responsibility for failure to exercise due diligence. In summary, as discussed in Section II, if State A has evidence of State B's failure to meet due diligence requirements, it can hold State B responsible for the omission. As mentioned, the two cyberattacks cited in the introduction *(Stuxnet* and *WannaCry)* can be viewed through this lens. As section II has explained, state B's failure to act is attributable to state B without difficulty: if the USA, Israel or North Korea failed to exercise due diligence in relation to *Stuxnet* and *WannaCry* respectively, state responsibility can be established for an omission. Attribution being simple, state A's challenges revolve 'only' around the determination of the scope of the relevant due diligence obligations and the comparison between those obligations and the conduct of state B. When analysing failures to exercise due diligence, attention turns toward the actions state B allegedly didn't take despite an obligation to do so. The analytical steps needed to establish state responsibility in such scenarios are entirely part of the customary structure of state responsibility. Consequently, due diligence does not operate beyond or in addition to the framework of state responsibility; rather, the emphasis is placed on different factors for omissions than for active conduct when we have to analyse if the conditions of state responsibility are met.

As we have demonstrated, state responsibility can as much pertain to a state's liability for its actions than for its omissions. When it comes to international law in cyberspace, this simple conclusion – already explicit in article 2 ARSIWA – does not yet seem to have been fully considered and explored, at least not in the most detailed Compendium of state positions published so far.

Another reason why the attribution of due diligence failures deserves more recognition in states' writings on cyberspace is to overcome the tendency to view the re-

sponsibility for omissions as an «indirect» form of state responsibility. As Jan Hessbruegge rightly summarises, «[t]he use of the term ‹indirect › is unfortunate»[76] when it comes to the attribution of failures to exercise due diligence over the conduct of non-state actors. Citing literature from the 1920s, Hessbruegge recalls that the responsibility of a state for its own active conduct and the responsibility of states for failing to exercise due diligence in preventing or reaction to conduct of non-state actors «have been referred to as direct and indirect responsibility» and that «[e]ven today, governments sometimes utilize this terminology, arguably because the latter term suggests a lesser degree of culpability to the lay observer».[77] Whether – or to what extent – states intend to indicate a lesser degree of «culpability» (or simply «responsibility» to avoid the very controversial debate about fault in the law of state responsibility) when they refer to «indirect» or «additional» forms of responsibility may remain open for further exploration in the context of cyber matters. Suffice it to say that the tendency to view the responsibility for omissions as a result of indirect attribution is still present, as evidenced in the Norwegian report where Norway states that due diligence was «of particular importance in a cyber context» when «a targeted State cannot *directly* attribute (technically and legally) a wrongful cyber operation».[78] Using the term «directly», suggests that due diligence would somehow serve to «indirectly» attribute cyber operations, but that is not the case. Rather, as mentioned, we attribute omissions and as we have seen, we do so «directly» by virtue of article 4 ARSIWA – as directly as we do for active conduct. Referring to «indirect» attribution or responsibility merely invites confusion and should be avoided.

Having clarified that failures to exercise due diligence are attributable in a straightforward way, the real challenges in the debate on due diligence in cyberspace concern the difficulties to clarify the scope of the various positive obligations of due diligence in the field of cyber activities. This is where, arguably, the most significant disagreements are to be resolved – disagreements that other authors have already discussed in much more detail than what is warranted here.[79] Suffice it to say that some states assert, erroneously in our view, that due diligence is merely a «voluntary, non-binding norm of responsible state conduct» within cyberspace (such as Can-

76 Jan Arno Hessbruegge, «The Historical Development of the Doctrines of Attribution and Due Diligence in International Law», 36 New York University of International Law and Politics (2004), 265–306, at 268.

77 Ibid.

78 Official Compendium, supra n. 6, Report by Norway, at 72 (our emphasis).

79 The Tallinn Manual 2.0 dedicates Rule 6 to the scope of due diligence obligations in relation to cyber operations: Tallinn Manual 2.0, supra n. 7, at Rule 6 and Commentary. For recent academic work, see notably Coco & De Souza Dias, supra n. 19, at 771; Delerue, supra n. 5, at chapter 8; Maria Monnheimer, Due Diligence Obligations in International Human Rights Law, Cambridge 2021, at 185–201; Anne Peters et al. (eds), Due Diligence in the International Legal Order, Oxford 2020.

ada,[80] Israel[81], New Zealand,[82] and the UK[83]), while others affirm due diligence as one or several binding obligations, but have various views about the legal nature of due diligence obligations in relation to cyber matters and the temporal and material scope of these obligations.[84] In this short article, we have observed that this recognition of the relevance of due diligence co-exists with a lack of elaboration on the attribution issues for due diligence failures. We thus conclude that states have at their disposal an attractive option to invoke state responsibility when another state allegedly fails to take measures required by international law. What remains to be done for states – and what is particularly controversial – is to spell out with more precision their positions about the scope of what they expect of each other in order to prevent, mitigate, limit and stop malicious cyber operations emanating from their territory. Of course, spelling out the various due diligence expectations means that states will expose themselves to be measured against their own standards. But so is the nature of international law and the necessity of deepening the discussion about the scope of the obligation(s) cannot be avoided. As Dan Efrony and Yuval Shany noted in 2018, «states show uneven interest in promoting legal certainty in cyberspace»[85] and the current geopolitical situation further complexifies the exercise of clarifying the substance of due diligence in cyber matters. Despite all difficulties, states can now build on the UN GEE 2021 report and the recent academic literature on due diligence which has shown that existing international law has considerable normative content to offer that seems relevant to cyberspace as well – including long before[86] a malicious cyber operation has started. Here, our contribution was limited to draw the attention of readers to how omissions are attributable for the purpose of state responsibility

80 Government of Canada, «International Law applicable in cyberspace», April 2022, para. 26, <www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng> (last accessed on 1 May 2023).

81 Roy Schondorf, «Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations», EJIL:Talk!, 9 December 2020, <hwww.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/> (last accessed on 28 April 2023).

82 New Zealand Foreign Affairs and Trade, «The Application of International Law to State Activity in Cyberspace», 1 December 2020, <www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf> (last accessed on 28 April 2023).

83 United Kingdom Foreign, Commonwealth & Development Office, «Application of International Law to States' Conduct in Cyberspace: UK Statement», 3 June 2021, para. 12, <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> (last accessed on 2 May 2023).

84 Talita Dias & Coco, supra n. 19, at 15.

85 Dan Efrony & Yuval Shany, «A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice», 112 American Journal of International Law (2018), 583–657.

86 «The majority of the International Group of Experts [elaborating the Tallinn Manual 2.0] was of the view that [due diligence] also applies to specific cyber operations that have not yet been launched». So are we. Tallinn Manual 2.0, supra n. 7, at 43.

and, importantly, what exactly we attribute. As things stand now for the Tallinn Manual 2.0, the international group of experts has formulated detailed rules on the scope of due diligence withing the domains in focus for the Manual.[87] One of these rules is entitled «compliance with the due diligence principle»,[88] but the Tallinn Manual 2.0 has not spelled out legal attribution for failures to exercise due diligence.[89] We recommend that this gap should be closed by states themselves when they update their state positions on international law in cyberspace. This is only a modest step towards further clarity on international law in cyberspace, but at least, our analysis has shown that states have at their disposal elegant and straightforward rules on the legal attribution of omissions.

87 Tallinn Manual 2.0, supra n. 7, at 4.

88 Tallinn Manual 2.0, supra n. 7, at Rules 6 and 7.

89 In the Tallinn Manual 2.0, there are various rules dealing with the attribution of cyber-related conduct to states (rules 15–18; including on complicity and control over non-state actors), but none of them on omissions of the state. Tallinn Manual 2.0, supra n. 7.