laws

MDPI

Article

Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications

Akiko Takano

Graduate School of Global Environmental Studies, Kyoto University; Kyoto 606-8501, Japan; takano.akiko.53c@st.kyoto-u.ac.jp

Received: 4 September 2018; Accepted: 29 October 2018; Published: 31 October 2018

Abstract: This paper analyzes the due diligence obligations with regard to transboundary harm in international water law and their application to cybersecurity by clarifying the definition of due diligence in light of the procedural duties in recent International Court of Justice (ICJ) cases. The paper explores whether states have responsibilities to prevent transboundary harm caused by nonstate actors. The existing literature on due diligence obligations in international water law and cybersecurity was reviewed, along with ICJ cases relating to procedural duties (international co-operation, environmental impact assessments, and information sharing). The findings confirm that, although procedural duties may be less onerous in cyberspace than in the environment, such duties indeed exist, albeit to a lesser degree. The differences may be accounted for by the fact that customary law related to the environment is already well developed. This study clarifies the concept of due diligence by focusing on procedural duties and examining the definition of due diligence in cyber operations. Due diligence obligations are crucial for states seeking to prevent transboundary harm and are an evolving principle of international law.

Keywords: due diligence; transboundary environmental harm; cybersecurity; procedural duties; international co-operation; impact assessment; nonstate actors

1. Introduction

The obligation to prevent significant transboundary harm is generally recognized as due diligence and is an evolving principle of international law (International Law Association (ILA) Study Group on Due Diligence in International Law, Second Report, July 2016, p. 47). Due diligence can be an important tool not only for dealing with traditional environmental issues, but also for responding to complex and novel legal issues, such as cybersecurity, by considering their global impact. Indeed, certain activities are increasingly borderless, with water security and cyberoperations both being among the most pressing issues requiring international co-operation to prevent significant transboundary harm. While transboundary harm may manifest itself differently in different scenarios, such as in the form of a wrongdoer (who is likely to be known in environmental cases but often unknown in cyberattack cases), wrongful acts ((un)intentional conduct vs highly likely intentional human actions), damage (environmental damage vs personal data theft, systems damage), and attribution (possible to identify vs difficult to identify), they all lead to seriously negative impacts for at least one other state.

Procedural duties can be an important factor when examining the concept of due diligence in cyberoperations and clarifying its role under customary international law. This is because procedural duties can lead to more objective, coherent, and stable interpretation. Indeed, due diligence is one of the most ambiguous terms in international liability and state responsibility (Kulesza 2016). Such vagueness is problematic because the nature and extent of state responsibility can be uncertain when states need to deal with issues of transboundary harm. It also raises concerns in terms of the possible application of due diligence to the private sector, as well as the obligation of state control of the private

sector, due to the crucial role of the private sector in cybersecurity. In addition, some states are hesitant to apply the due diligence principle to cyber activities due to the corresponding obligations that would be imposed on them (Schmitt 2015).

This paper first elucidates the definition of due diligence in the context of transboundary environmental harm in order to clarify and consolidate the concepts underlying the due diligence standard. Second, the paper examines exactly what the due diligence obligations of states are in regard to securing their networks and prosecuting cyber attackers (Taddeo and Glorioso 2017). Finally, the paper analyzes what the principle of due diligence would require states to do in order to prevent harmful acts from arising from the private sector, and whether states can place demands on the private sector in light of its significance in protecting cybersecurity (Kulesza 2016).

2. Due Diligence in International Environmental Law

2.1. Due Diligence Obligations

States have the sovereign right to exploit their own resources in accordance with the Charter of the United Nations and the principles of international law, as well as the responsibility to ensure that activities within their jurisdiction do not cause harm to the environment of other states[1]. "Due diligence" is one of the key concepts in international law to mediate interstate relations when there is significant change (International Law Association (ILA) Study Group on Due Diligence in International Law, First Report, March 7, 2014, p. 2). Due diligence is normally assessed if a responsible state has complied with certain obligations and standards (Max Planck Encyclopedia of Public International Law [*MPEPIL*], Due Diligence, Timo Koivurova, February 2010). However, "certain obligations and standards" are internationally not defined and considered flexible (Kulesza 2016), and would vary depending on the circumstances of the case (International Law Association (ILA) Study Group on Due Diligence in International Law, First Report, March 7, 2014, p. 2). Consequently, more detailed rules have been developed, particularly in environmental areas, which include the "no-harm principle" in customary international law (Max Planck Encyclopedia of Public International Law [*MPEPIL*], Due Diligence, Timo Koivurova, February 2010). Indeed, scholars consider that customary law manages state responsibilities in transboundary harm (Max Planck Encyclopedia of Public International Law [*MPEPIL*], Due Diligence, Timo Koivurova, February 2010), while the term "due diligence" is seldom seen in international treaties (International Law Association (ILA) Study Group on Due Diligence in International Law, First Report, March 7, 2014, p. 2).

Due diligence obligations may not have "unified content", so it may be difficult to identify core features of the due diligence obligation, but the material contents of the due diligence obligation could be defined with particular reference to customary law when states use their capacity to prevent their cyberinfrastructure from being used by nonstate actors as a place to perform malicious transboundary activities (Buchan 2016).

2.2. Do-No-Harm Principles

Due diligence obligations have significantly arisen in areas of transboundary environmental harm (Kulesza 2016). In international environmental law, due diligence is an important component of the obligation to prevent transboundary harm. This obligation requires states to take measures to protect persons or activities beyond their respective territories in order to prevent harmful events and outcomes[2]. The International Court of Justice (ICJ) confirmed the customary nature of this principle

---

1 Rio Declaration on Environment and Development, Rio de Janeiro, 14 June 1992. Principle 2.

2 Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, UN 2001, Commentary to Art 3, 154, para (7). In addition, the Convention on the Law of the Non-Navigational Uses of International Watercourses Adopted by the General Assembly of the United Nations on 21 May 1997, Article 7—Obligation Not to Cause Significant Harm, and the Convention on the Protection and Use of Transboundary Watercourses and International Lakes (Water

in 1949 in *Corfu Channel*[3] when referring to a state's obligation to not knowingly allow its territory to be used for acts contrary to the rights of other states. The Draft Articles on the Prevention of Transboundary Harm from Hazardous Activities (ILC)[4] also indicate that states have a duty to prevent significant transboundary harm (Article 3) and provide an assessment of possible transboundary harm (Article 7). Moreover, the *Trail Smelter* (*United States* vs. *Canada*) case asserts the following:

> No State has the right to use or permit the use of its territory in such a manner as to cause injury by the emission of fumes in or transported to the territory of another or the properties or persons therein, when the case is of serious consequence and injury is established by clear and convincing evidence[5].

Thus, the "do-no-harm principle" has been widely recognized as customary law, particularly in the context of shared resources such as international water. Furthermore, Principle 21 of the Stockholm Declaration[6] and Principle 2 of the Rio Declaration[7] provide the legal basis of the international standard. With regard to whether the do-no-harm principle requires a duty to prevent all significant transboundary harm, as the Advisory Opinion on the *Legality of Nuclear Weapons*[8] and the *Gabcikovo–Nagymaros*[9] case indicate, states are only required to prevent harm caused as a result of an active disposition on or over their territory, which does not include the omission of protective measures. This principle of no harm is breached only when the state of origin has not acted diligently with regard to its own activities over state-owned enterprises or private activities (International Law Association (ILA) Study Group on Due Diligence in International Law, First Report, March 7, 2014, p. 2,). According to the Draft Articles on the Prevention of Transboundary Harm from Hazardous Activities[10], the Commentaries stated that the duty measured to prevent or minimize activities is one of due diligence, and the due diligence standard regarding transboundary environmental harm should be examined on whether the standard considered is appropriate and proportional to the risk of transboundary harm in the particular instance.

The *Genocide*[11] case also made it clear that the due diligence obligation is one of conduct and not one of result. This results in the principle of due diligence being an obligation of conduct, rather than an obligation to achieve a result (Kulesza 2016); that is, states are not required to achieve specific results as long as states exercise the best possible efforts to obtain the results. If a state fails to take "all reasonable or necessary measures to prevent" harm, then the states are liable for their conduct, not the result of harm (Buchan 2016).

In order to demonstrate its best possible effort, the state of origin is requested to prevent foreseeable significant damage, or at least minimize the risk of such harm (International Law Association (ILA) Study Group on Due Diligence in International Law, First Report, March 7, 2014, p. 2)[12]. According to Seabed Mining Advisory Opinion, precaution is "an integral part of the general obligation of due diligence"[13], and states may be requested to act, including creating a legislative and

---

Convention), adopted in Helsinki on 17 March 1992, the United Nations Economic Commission for Europe, Article 3 Prevention, Control and Reduction.

3 *Corfu Channel Case* (*UK v Albania*) (Merits) [1949] ICJ Rep. 4.

4 Draft articles on Prevention of Transboundary Harm from Hazardous Activities, supra note 2.

5 Reports on International Arbitral Awards, *Trail Smelter case* (*United States, Canada*), 16 April 1938 and 11 March 1941, vol. III, pp. 1905–82.

6 Declaration of the United Nations Conference on the Human Environment, Stockholm, 16 June 1972.

7 Rio Declaration on Environment and Development, supra note 1.

8 *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, [1996] ICJ Rep. 1996 (I), 241–42, para 29.

9 *Case concerning the Gabcikovo–Nagymaros Project* (*Hungary/Slovakia*), ICJ Rep. 1997 41, para 53.

10 Draft articles on Prevention of Transboundary Harm from Hazardous Activities, supra note 2.

11 Application of the *Convention on the Protection and Punishment of the Crime of Genocide* (*Bosnia v Serbia*) (Judgment) [2007] ICJ Rep. 1, para 430.

12 Also, *Pulp Mills on the River Uruguay* (*Argentina v Uruguay*) [2010] ICJ Rep. 14, para 101.

13 *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area* [ITLOS Advisory Opinion, Seabed Chamber] (Seabed Dispute Chamber of the International Tribunal of the Law of the Sea, Case No 17, 1 February 2011), para 131.

regulatory framework regardless of insufficient evidence, as long as the consequences are foreseen under the precaution principle (International Law Association (ILA) Study Group on Due Diligence in International Law, First Report, March 7, 2014, p. 2).

In terms of state responsibilities, it is not necessary for all states to take similar measures against foreseen consequences because due diligence obligations may be imposed according to "their capabilities"[14], considering the differences in their economic and technological development stages. However, such different treatment has the limitation of avoiding a situation to "jeopardize uniform application of the highest standards of protection of the marine environment", as well as to avoid states' convenience[15].

2.3. Emergence of Procedural Duties

In order for states to meet their due diligence obligations, they have to establish various domestic and transboundary procedures to prevent significant transboundary damage. A breach of procedural obligations constitutes a critical component in establishing a lack of due diligence standards, as required under the customary duty to prevent significant transboundary harm (Dupuy and Viñuales 2015). *Pulp Mills*[16] is a landmark decision clarifying the relationship between the procedural and substantial rules of international environmental law under the customary duty to prevent transboundary harm (McIntyre 2011). It confirms that procedural obligations are an integrated and indivisible whole, and that procedural obligations exist separately from substantial obligations (McIntyre 2011). The Advisory Opinion of the Seabed Chamber[17] also suggests that the due diligence obligation is a conceptual bridge between harm prevention and precaution (Brunnée 2016). Having considered case development and the importance of procedural rules, it may be presumed that an active implementation of procedural obligations would strengthen the application of a substantial obligation, making it crucial to consider the evolution of cases in this regard.

The importance of procedural law is also evident in some provisions of the Convention on the Law of the Non-Navigational Uses of International Watercourses (UN Watercourse Convention, or UNWC), such as Part II—General Principles, Article 8—General Obligation to Co-Operate, and Article 9—Regular Exchange of Data and Information[18]. In addition, procedural duty has the potential to strengthen the aspects of the prevention of the transboundary harm principle, which supports the due diligence standard (Brunnée 2016).

The "duty to co-operate" is an essential procedural duty that includes the duty to notify and consult with the concerned states, the obligation to conduct an environmental impact assessment (EIA), and the principle of prior informed consent. The first step in the process of co-operation to prevent transboundary harm is the exchange of scientific data and information to protect the environment and ecosystems. The EIA also plays a pivotal role in relation to notification; therefore, conducting a transboundary EIA is an essential and independent obligation in international law in cases where significant transboundary harm is expected (Brunnée 2016). The ICJ indicates that simply having laws in place to prevent environmental harm is in and of itself insufficient in terms of exercising a standard of due diligence[19]. States have the duty to notify neighboring states as soon as a plan of construction is received, and then send a more detailed notification to neighboring states on the basis of an EIA (McIntyre 2011).

---

[14] Ibid., para 161.
[15] Ibid., para 159.
[16] *Pulp Mills*, supra note 12, para 101.
[17] ITLOS Advisory Opinion, Seabed Chamber, supra note 13.
[18] Convention on the Law of the Non-Navigational Uses, supra note 2.
[19] *Pulp Mills*, supra note 12.

As to the form of the notification[20], on the one hand, customary law requires it to be in good faith, and it should include information regarding the nature of the activity, its risks, and potential injury to the state and watercourse. It is expected that the notification will be sent within a reasonable amount of time to allow for a response to be made, and it includes an obligation to consult in good faith. During the consultation, the notifying state cannot undertake the proposed activities unless they are urgent and have been declared as such. Similarly, as a matter of good faith, another state may not prevent the notifying state from undertaking the planned activities by simply not responding (Dupuy and Viñuales 2015).

2.4. Some Modifications of Procedural Obligations

However, following such a development—that is, procedural obligations that are an integrated and indivisible whole—the ICJ did not take "a progressive approach" (Brunnée 2016) to its understanding of the due diligence obligation in light of the risk threshold to trigger an EIA obligation. While an EIA was considered to be an essential element of the due diligence obligations, in *Costa Rica* vs *Nicaragua*[21] the court found that no EIA was necessary because the dredging program had a limited scope and the program did not pose a risk of significant transboundary harm[22].

It concluded that Nicaragua was not required to notify or consult with Costa Rica because it was not under an obligation to conduct an EIA, given the absence of a risk of significant transboundary harm[23]. Therefore, it would be useful to view the criteria for "the absence of risk" regarding the obligation to conduct an EIA under the procedural obligations of due diligence duties for cybersecurity issues.

3. Due Diligence in Cyberspace

3.1. Cybersecurity

States, entities, and individuals heavily use computer and information and communication technologies (ICT), and ICT are central to modern society (Gross 2015). Cybersecurity is high on the agenda for all sectors, and cyber risks present critical strategic challenges for leaders[24]. After the Sony hack in 2014 (Sullivan 2016), the cyberattack was declared a "national emergency" in the United States in January 2015; this was followed by another incident of Russia possibly hacking the U.S. election in October 2016 (Fidler 2017). As these incidents show, cyberattacks are a threat to international peace and security (Kulesza 2009).

The number of cyberattacks against states is increasing, and they are becoming more sophisticated[25]. In addition to cyberattacks, cyberespionage and cyberwarfare are also cybercrimes. While cyberattacks and cyberespionage may be intentional, cybersecurity incidents may occur unintentionally as a result of human error (Gross 2015). These cyberspace incidents are not controlled by effective and specific treaty-based rules because states and nonstate actors tend not to regulate their behavior to take advantage of such situations (Zimmermann 2014). In addition, cyberspace would

---

[20] The notification is described in Rio Principle 19; Stockholm Declaration 51(b)(i), UNECE Conv. Art. 9(2)(h), UNWC Arts. 11–19 (Part III: Planned Measures) and is analyzed in the *Lac Lanoux* Arbitration (*France v Spain*), (1957) 12 R.I.A.A. 281; 24 I.L.R. 101, Arbitral Tribunal. 1 November 16, 1957 (Petrén, President; Bolla, De Luna, Reuter, De Visscher), *Gabcikovo*, supra note 9, and Pulp Mills, supra note 12.

[21] 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, *ICJ Rep*. 2015, p. 665.

[22] Ibid., para 105.

[23] Ibid.

[24] World Economic Forum, "Advancing Cyber Resilience: Principles and Tools for Boards", January 2017, p. 4–5.

[25] BIICL, "State Responsibility for Cyber Operations: International Law Issues Event Report", 9 October 2014. p. 1. https://www.biicl.org/documents/380_biicl_report_-_state_FFresponsibility_for_cyber_operations_-_9_october_2014.pdf?showdocument=1 (accessed on 15 October 2018).

make it more difficult to have agreeable international treaties due to specific technical features of ICT, including rapid technical development as well as technical gaps between states (Zimmermann 2014).

In terms of attribution, states generally have responsibilities only if conduct that is attributed to a state constitutes a breach of one of its international obligations, because attribution establishes a nexus between an act through a physical person and the state[26]. Attribution is a complicated issue in general, and more demanding in cyberspace due to anonymity, the possibility of multistage action (different persons, places, and jurisdictions), and the speed of operation[27]. Here, the modality of state responsibilities under due diligence obligations can be an answer to tackle such challenges (Jolley 2017): states are responsible for cyberattacks originating from within their sovereign territories under strict liability as an accepted norm in customary international law as an alternative choice, since the application of existing customary international law is very difficult, yet attributing responsibilities is imperative (Jolley 2017).

Further extension of this theory may be possible, that is, even transiting states whose cyberinfrastructure is being used in their territories for malicious cyber conduct have an obligation to prevent their territories from being used by referencing the ICJ *Nicaragua* case[28], in which their territory was used as a trafficking route for military equipment (Buchan 2016). However, a challenge in cyberspace is that identifying the source is extremely difficult, if not impossible, when it is malicious (Gross 2015), while it is contrarily claimed that the attribution of malicious actions is becoming increasingly possible for a few countries that possess advanced technologies (Lewis 2016).

3.2. Comparison of Cyberspace and Environment

Due to cross-border interconnectivity, both the environment and cybersecurity have several similar features, and they might help to define and apply due diligence obligations, which is a flexible concept, as described earlier. The first area to compare is sovereignty. Cyberspace used to be considered in areas where traditional rules and principles of international law do not apply, whereas in recent state practice, customary international law is, in principle, applicable to cyberspace with some adaptation to the specific characteristics of cyberspace (Von Heinegg 2013). Such applicability is particularly important because cyberspace lacks a major intergovernmental governance structure (Zimmermann 2014).

Cyberspace is also not immune from state sovereignty claims, and states have imposed the obligation to prevent transboundary harm toward activities occurring within their sovereign territory (Buchan 2016). In terms of state responsibility, on the one hand, neighboring countries are likely to suffer in the case of environmental issues, such as water pollution, or it may take time in the long term to suffer or recover from negative consequences, such as nuclear disaster and climate change. On the other hand, in the case of cybersecurity, states have to consider the instant spillover to other states because of network connectivity, so states may be required to take immediate action to protect individuals' rights under the notion of sovereignty and human rights laws in cases of data theft, since such incidents may invade the privacy or basic rights of individuals (Gross 2015). In particular, there appear to be stronger privacy concerns for collection of information to share to other states in cyberspace. However, recovering from the damage of the system itself may be quicker except for the invasion of privacy.

Significant transboundary environmental harm may affect the physical or nonphysical, such as with financial loss and damage to natural resources, which states are expected to manage, whereas cyberattacks may result in serious risks to national infrastructure, financial loss, and nonphysical risks

---

[26] Ibid., p. 2.
[27] Ibid., p. 2.
[28] *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v United States of America*) (Merits) [1986] ICJ Rep. 14, para 157.

such as privacy, and possibly physical risks, as they "endanger their health and lives" (Gross 2015). Therefore, there do not appear to be significant differences for either.

It would be possible to consider that the environment and ICT are of "common concern to humanity" because both are essential for most, if not all, people. While only sovereign territories become an issue in the environment, in cybersecurity, not only are state territories used for launching cyberattacks, but they are also possibly extended to directly affected states that brought risks to their nations and other states and nonstate actors (Gross 2015).

3.3. Cyberdiligence

States have a due diligence obligation to not knowingly allow their territories to be used for internationally wrongful acts using information and communication technologies[29], and states have an obligation to prevent cyberattacks from originating from within their borders (Liu 2017).

With regard to cyber diligence, Rule 6 of the Tallinn Manual 2.0, prepared by the International Groups of Experts at the invitation of the NATO Co-Operative Cyber defense Centre of Excellence, indicates that the due diligence principle can apply to cyberoperations (Schmitt and Vihul 2017). However, the manual does not clearly indicate what kinds of action drive the due diligence principle (Hankinson 2017). Unlike real-world cases, such as the prohibition of chemical weapons or the discharge of harmful substances under environmental law, it may be difficult and complicated to prohibit the use of cyberweapons under international law due to certain technical challenges and verification hurdles (Shackelford 2014).

The question is what the principle of due diligence would require states to do in terms of their cyber infrastructure, cyber activity, and people engaged in cyber activities. As mentioned above, regardless of the global connectivity of the Internet, cyberspace is no longer seen as a unique space and national law applies to networks, at least when they are located in a state's territory[30]. However, when the principle applies to cybersecurity, specific obligations may be required due to the lack of internationally established law, as well as the different features between cybersecurity and environmental cases. Such differences in cybersecurity can include who the wrongdoer is (often unknown), the types of wrongful acts (highly likely to be intentional human actions), the damage (personal data theft and damage to systems), and attribution (the difficulty of identifying those responsible). Consequently, the concept of due diligence in environmental law and the law of the sea may not be directly applied to cybersecurity (Liu 2017). In addition, it could be said that cyberspace contains higher risks than environmental cases. As a result, the standard of a due diligence obligation may be higher[31].

3.4. Preventive Action

A note from the UN Group of Governmental Experts (GGE) indicates the importance of procedural obligations to prevent harm, and encourages states to co-operate "to mitigate malicious ICT activity emanating from their territory"[32]. States may be expected to discharge their due diligence obligations and have a defense system for cybersecurity incidents (Gross 2015). Due diligence obligations request the monitoring of activity implementation, namely, the "exercise of administrative control applicable to public and private operators, such as the monitoring of activities undertaken by such operators"[33].

---

[29] UN, General Assembly, A/70/174 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General, 22 July 2015, p. 16.
[30] Ibid., p. 10.
[31] ITLOS Advisory Opinion, Seabed Chamber, supra note 13, para 117.
[32] UN, General Assembly, A/70/174, Developments in the field of information and telecommunications in the context of international security Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Section 17(e), https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf (accessed on 20 October 2018).
[33] *Pulp Mills*, supra note 12, para 197.

States also have an obligation to monitor cyber activities in their territories (Bannelier-Christakis 2015). Indeed, the states' duty to better monitor the Internet in their respective territories is triggered by the state sovereignty principle (Jolley 2017). While such monitoring may lead to concerns in relation to privacy, states are also under obligation to respect the right to privacy when monitoring activities, as it was confirmed in the *Genocide* case[34] and the UN General Assembly[35] (Buchan 2016).

In addition, states have an obligation to stay informed about cyberattack threats occurring in their territories (Buchan 2016). Early warning systems against cyberattack threats may supplement such a warning system. Several monitoring systems exist on an international level to safeguard against threats in different areas, such as the International Atomic Energy Agency (IAEA)[36], which have achieved certain results. According to Article 5 of the Prevention of Transboundary Harm from Hazardous Activities 2001[37], states "shall take the necessary legislative, administrative or other action including the establishment of suitable monitoring mechanisms..." Indeed, monitoring may be an effective measure because firewalls and antivirus programs (traditional forms of security) may no longer be enough to prevent advanced cyberthreats.

The monitoring system may be included to produce warnings against cyberthreats and security incidents (Gross 2015), as well as monitoring all activities in the network across a state's territory. One example may be to have an international monitoring system conducted by an international organization under the basis of a treaty like IAEA or OPCW, or domestic authorities conducting 24 h monitoring with other authorities over cyber threads (Buchan 2016) under bilateral or multilateral agreement, or even on a voluntary basis as a co-operation. Monitoring by international organizations may be particularly useful to those who lack technical and financial capabilities (Gross 2015).

Due to the connectivity and global nature of cyberspace, it may be concluded that there is a higher risk of transboundary harm. However, there has been no development in the discussion of impact assessments as they apply to cyberspace. Without an EIA, it is difficult to judge whether states fulfill their due diligence obligations in terms of (preventing) transboundary water pollution. Thus, all states should conduct impact assessments to prevent significant transboundary harm as it applies to cybersecurity. In the recent real-world decision of *Costa Rica* vs *Nicaragua*[38], it was confirmed that, if there is no significant harm, an EIA is not required. If this also applies to cybersecurity, it may prove too late to prevent a large cyberattack, because the speed and scope of the harm would be much faster and broader. Consequently, the standard set in *Pulp Mills*[39] may be desirable; that is, the failure to conduct an EIA and an action amounting to a lack of due diligence would constitute a violation of the duty to prevent harm.

3.5. Information Sharing and Security

As discussed, information sharing is an important procedural obligation found under the due diligence principle. The issue is which kinds of information sharing (including intelligence and details about the crime) are necessary, and at which stage such information is required to be exchanged. Information sharing is the first step towards parties' co-operation in general. However, national security concerns can impose limitations on information sharing, in particular on obtaining information relating to real-time situations (Gross 2015). These concerns may have a greater impact on the limitation of

---

34 *Genocide*, supra note 11, para 430.
35 UNGA Res 68/167 'The Right to Privacy in the Digital Age' (18 December 2013) UN Doc A/RES/68/167.
36 Convention on Early Notification of a Nuclear Accident, adopted by the UN General Conference at its special session, 24–26 September 1986, and was opened for signature at Vienna on 26 September 1986 and at New York on 6 October 1986. It establishes a notification system for nuclear accidents from which a release of radioactive material occurs or is likely to occur and which has resulted or may result in an international transboundary release that could be of radiological safety significance for another State. (https://www.iaea.org/topics/nuclear-safety-conventions/convention-early-notification-nuclear-accident, accessed on 19 October 2018).
37 Draft articles on Prevention of Transboundary Harm from Hazardous Activities, supra note 2.
38 *Costa Rica*, supra note 21.
39 *Pulp Mills*, supra note 12.

sharing information than they would in the case of environmental law, regardless of the importance of information sharing. Moreover, it would be difficult to collect personal information (which is held by the private sector) and share it with other states, even in cases of serious transboundary harm, because of privacy concerns.

Although there are potentially huge limitations, an open and uninterrupted channel of information sharing and communication with other states and possibly with nonstate actors remains important (Gross 2015). Considering the essential role of nonstate actors, it would be effective for and in the interests of both states and the private sector to create stronger safeguards against cyber incidents (Gross 2015). Nonstate actors also have contractual obligations with their clients, a duty of care to have a secure network for their data, and a fiduciary duty to keep their data secure (Gross 2015). Therefore, creating "networks" within and beyond states seems to be useful and potentially essential to ensure that it does not jeopardize national security, as well as maintaining independence from each other. Timely information sharing is becoming increasingly essential to fighting against cyberattacks. Exchanging information about actual criminal activity may be possible only when both states agree to co-operate, and such co-operation should be much encouraged.

3.6. Nonstate Actors

The private sector plays a key role in cyberspace, that is, it has de facto control over most Internet infrastructure, and more than 90% of the U.S. critical national Internet infrastructure is in private hands (Shackelford 2014). However, states are not generally responsible for the conduct of nonstate actors that cause harm to other states due to a territorial link alone (Buchan 2016). As seen in the Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, and in the Gabcikovo–Nagymaros Project, states are required to act to prevent significant transboundary harm where such harm is caused by a disposition over their territory, where such states have an opportunity to do so, and where it is foreseeable that the disposition would cause significant transboundary harm and the measures required to prevent such harm are proportionate (Bremer 2017).

Where activities are conducted by a private person or enterprise, the obligation of the state is "establishing the appropriate regulatory framework and applying it."[40] This may be an "absolute obligation" to prevent their territories from being used, violating their legal rights under customary law (Buchan 2016). This obligation is critical to preventing and punishing cybercrime, but its effectiveness may be limited since states have discretion on what regulations they create and how to control cyberspace. As stated above, it is difficult to identify attribution of cyberattacks, and specific efforts by states are required to prevent serious damage from originating from within their state territory. According to IGE, states have obligations to ensure that their territories are not used by nonstate actors for unlawful use, and this due diligence obligation is imposed by states and governments to private cyberinfrastructure on their territory and cyber activities emerging from that territory (Gross 2015).

Individuals acting within a state's jurisdiction are required to respect due diligence obligations. States can request that the private sector follows their domestic laws[41]. Therefore, states should pass national laws that reflect the international consensus and are supported by solid technical knowledge (Kulesza 2016). The UN GGE also indicates which of the principles of the UN Charter and international law apply to states[42]: states must not use proxies to commit internationally wrongful acts using information and communications technologies, should seek to ensure that their territory is not used by

---

[40] Ibid. Commentary to Article 5, p. 156.

[41] International Law Association (ILA) Study Group on International Law and Cyberterrorism, Study Group Report, 31 July 2016, p. 62, available at http://cyberregstrategies.com/wp-content/uploads/2017/03/ILA_SG_Cyber_Terrorism_FINAL_REPORT.pdf (accessed on 13 June 2018).

[42] UN, General Assembly, A/70/174, supra note 32. Forward.

nonstate actors to commit such acts, and must take responsibility for internationally wrongful acts attributed to them under international law[43].

As a result, a state can incur responsibility when it fails to satisfy its primary obligations, whether conventional or customary, to take positive action in relation to the conduct of a nonstate actor operating within its territory or, more broadly, any actor that is subject to its jurisdiction or legislative framework. Indeed, experts agree that states have a due diligence obligation in terms of the government and private cyberinfrastructure and cyber activities in their territory: if a state fails to meet its due diligence obligations, a victim state can claim a right to legal remedies when appropriate (Schmitt 2015). In other words, although the due diligence obligation under customary international law may not be directly applicable to the private sector, states have an obligation to ensure that nonstate actors under their jurisdiction obey international law. The state is required to take measures to terminate a wrongful act and mitigate transboundary harm. Therefore, it can be concluded that the private sector has an "indirect" obligation to respect its due diligence obligations under customary law in terms of cybersecurity if states impose obligations to the private sector in their domestic law to an equal or even higher degree of obligations.

3.7. International Co-Operation beyond Due Diligence

Public international law plays an essential role in regulating activities in cyberspace (Kittichaisaree 2017). Since cybercrime tends to be crime of a global nature, it requires a global legal regime. However, states take different positions on whether cyberspace is a new area that requires new law. Indeed, the field of international cybersecurity law remains relatively immature, and states have not yet developed international law to protect essential infrastructure, regardless of a widespread policy emphasis on cybersecurity protection[44]. Given the rapid development of cyber capabilities, there are comparatively few treaties that specifically address the rights and obligations of the state. The exception to this is the Convention on Cybercrime (the Budapest Convention)[45], which is the first—and currently the only—binding international legal instrument on crimes committed via the Internet and other computer networks. Its objective is "to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation"[46]. While 59 states have ratified it[47], China, a nonparty of the Budapest Convention, claimed that the state parties would not be willing to share sensitive information (Kittichaisaree 2017).

Co-operative efforts may be limited to agreements among politically aligned states (Liu 2017). The UN GGE identifies the voluntary, nonbinding norms[48] for responsible state behavior to create an international code of conduct for information security. The Tallinn Manual (Schmitt and Vihul 2017) is based on a Euro–Atlantic consensus on law in cyberspace and has not been generally accepted by the international community (Giles 2017). The United States and China signed a bilateral agreement in 2015 concerning economic espionage, reflecting a trend in bilateral and regional implementation that may be more effective in terms of immediacy than developing an international agreement. Although the creation of an internationally binding agreement or cybercrime convention may be very difficult due to developments being made in both technology and national security, it would be beneficial to establish an international cyberattack monitoring and warning system, because they are intentional

---

43 Ibid., para 28 (e). Also see International Law Commission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries' (2001). http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf (accessed on 16 October 2018).

44 ILA Study Group Report on International Law and Cyberterrorism, supra note 41, p. 69.

45 The Convention on Cybercrime of the Council of Europe (CETS No. 185) (2001).

46 Ibid. Preamble.

47 Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime, Status as 16 June 2018 available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (accessed on 16 June 2018).

48 UN, General Assembly, A/70/174, Supra note 32, para 2.

human acts. Moreover, greater co-operation, including information sharing, between governments and the private sector would be very useful in terms of finding technical solutions.

4. Conclusions

This study clarifies the concept of due diligence by focusing on procedural duties and examining the definition of due diligence in cyberoperations. Due diligence obligations are crucial for states to prevent transboundary harm and are an evolving principle of international law. States tend to engage in co-operation when opportunities exceed the risks and benefits outweigh the costs. Taking procedural obligations into account, such opportunities would lead to a more objective, coherent, and stable interpretation of due diligence concerning transboundary environmental pollution and cybersecurity. Having applied the standard of due diligence in transboundary environmental harm to cybersecurity, this study developed further understanding of the due diligence obligation standard.

While procedural duties may be paid less attention in cyberspace than in the environment, such duties indeed exist, and they are a critical element to prevent cyber damage considering the technical nature, speed, and interconnectivity. The fact that customary law is well developed in the area of the environment, and that the UN Water Convention has already been established, may account for the differences.

States are trying to take stricter measures to prevent and punish abuses of the use of cyberspace. Developing appropriate legislation, strategies, and regulatory frameworks may substitute due diligence obligations under customary law to nonstate actors. Regardless of technical capacity, all states should have the same due diligence obligations since they are not required to take measures that are beyond their means or otherwise unreasonable (Schmitt 2015) and given the connectivity of cyberspace with other countries. Understanding that there is a huge gap in terms of technical and economic development among states makes international co-operation essential in this regard.

Due diligence of transboundary harm in environmental law is a developing concept and can be adapted to the new digital age. As in the case of environmental harm, from a transborder perspective, the due diligence principle is applicable to cyberspace considering its unique nature. Although creating internationally binding agreements seems difficult, it would be useful to develop procedural obligations, such as cyberattack monitoring and warning systems, as well as notifications. Since all states have a due diligence obligation to prevent transboundary harm under customary law, they are required to ensure that activities within their jurisdiction do not cause harm to other states or areas beyond their national jurisdiction, and rapid international co-operation seems to be the key for the successful prevention of cyber incidents.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

Bannelier-Christakis, K. 2015. Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations? *Baltic Yearbook of International Law Online* 14: 23–39. [CrossRef]

Bremer, Nicolas. 2017. Post-environmental impact assessment monitoring of measures or activities with significant transboundary impact: An assessment of customary international law. *RECIEL* 26: 80–90. [CrossRef]

Brunnée, Jutta. 2016. Procedure and substance in international environmental law: Confused at a higher level? *ESIL* 5: 1–7.

Buchan, Russell. 2016. Cyberspace, non-state actors and the obligation to prevent transboundary harm. *Journal of Conflict and Security Law* 21: 429–53. [CrossRef]

Dupuy, Pierre-Marie, and Jorge E. Viñuales. 2015. *International Environmental Law*. Cambridge: Cambridge University Press.

Fidler, David. 2017. The U.S. Election Hacks, Cybersecurity, and International Law. *Articles by Maurer Faculty* 110: 337–42. [CrossRef]

Giles, Keir. 2017. *Prospects for the Rule of Law in Cyberspace*. Carlisle: Strategic Studies Institute and U.S. Army War College Press.

Gross, Oren. 2015. Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents. *Cornell International Law Journal* 48: 481.

Hankinson, Olivia. 2017. Due diligence and the gray zones of international cyberspace laws. *MJIL* 39: 1–21.

International Law Association (ILA) Study Group on Due Diligence in International Law, First Report, March 7, 2014, p. 2. Available online: https://olympereseauinternational.files.wordpress.com/2015/07/due_diligence_-_first_report_2014.pdf (accessed on 15 October 2018).

International Law Association (ILA) Study Group on Due Diligence in International Law, Second Report, July 2016, p. 47. Available online: http://www.ila-hq.org/index.php/study-groups (accessed on 21 June 2018).

Jolley, Jason D. 2017. Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law. Ph.D. thesis, University of Glasgow, Glasgow, UK. Available online: https://ssrn.com/abstract=3056832 (accessed on 11 October 2018).

Kittichaisaree, Kriangsak. 2017. *Public International Law of Cyberspace*. Cham: Springer.

Kulesza, Joanna. 2009. State Responsibility for Cyber-Attacks on International Peace and Security. *Polish Yearbook of International Law* 29: 139–52.

Kulesza, Joanna. 2016. *Due Diligence in International Law*. Nijhoff: Brill.

Lewis, James. 2016. *Report of the International Security Cyber Issues Workshop Series*. Working Paper. Geneva, Switzerland: United Nations Institute for Disarmament Research (UNIDIR), Center for Strategic & International Studies (CSIS).

Liu, Ian Yuying. 2017. State responsibility and cyberattacks: Defining due diligence obligations. *The Indonesian Journal of International and Comparative Law* 4: 191–260.

McIntyre, Owen. 2011. The world court's ongoing contribution to international water law: The *Pulp Mills* case between Argentina and Uruguay. *Water Alternatives* 4: 493–94.

Max Planck Encyclopedia of Public International Law [MPEPIL], Due Diligence, Timo Koivurova, February 2010. Available online: http://opil.ouplaw.com/abstract/10.1093/law:epil/9780199231690/law-9780199231690-e1034?prd=EPIL (accessed on 16 October 2018).

Schmitt, Michael N. 2015. In defense of due diligence in cyberspace. *The Yale Law Journal* 125: 68–81.

Schmitt, Michael N., and Liis Vihul, eds. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

Shackelford, Scott J. 2014. *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*. Cambridge: Cambridge University Press.

Sullivan, Clare. 2016. The 2014 Sony Hack and the Role of International Law. *Journal of National Security Law and Policy* 8: 437–68.

Taddeo, Mariarosaria, and Ludovica Glorioso, eds. 2017. *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative*. Basel: Springer.

Von Heinegg, Wolff Heintschel. 2013. Territorial Sovereignty and Neutrality in Cyberspace. *International Law Studies* 89: 122–156.

Zimmermann, Andreas. 2014. International law and "Cyber Space". *European Society of International Law (ESIL) Reflection* 3: 1–6.