CHARLES UNIVERSITY

Faculty of Law

Adam Botek

The Application of the Due Diligence Principle in Cyberspace

Master's Thesis

Master's thesis supervisor:

doc. JUDr. PhDr. Veronika Bílková, Ph.D., E.MA.

Department of International Law

Date of completion (manuscript closure): 14. 4. 2020

UNIVERZITA KARLOVA

Právnická fakulta

Adam Botek

Aplikace principu náležité péče v kybernetickém prostoru

Diplomová práce

Vedoucí diplomové práce:

doc. JUDr. PhDr. Veronika Bílková, Ph.D., E.MA.

Katedra mezinárodního práva

Datum vypracování práce (uzavření rukopisu): 14. 4. 2020

Declaration

Hereby, I declare that this master's thesis is my original work and that I have written it independently. All sources and literature that I have used during elaboration of the thesis are fully cited and listed. I further declare that this thesis has not been used to obtain any other or the same degree.

The text of this thesis has 183 406 characters including spaces and footnotes.

Adam Botek

In Prague on

Prohlášení

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 183 406 znaků včetně mezer.

Adam Botek

V Praze dne

Acknowledgement

I would like to thank my thesis supervisor, doc. JUDr. PhDr. Veronika Bílková, Ph.D., E.MA. for inspiring discussions and her valuable comments and supportive attitude during my work on this master's thesis. I would also like to express my gratitude to JUDr. Tomáš Minárik, Head of International Organisations and Law Unit at Czech National Cyber and Information Security Agency, for his expert advice since the very beginning of my work on the thesis. Last but not least, I would like to sincerely thank my family and my girlfriend for their endless support in the course of my studies.

Poděkování

Chtěl bych poděkovat vedoucí mé práce paní doc. JUDr. PhDr. Veronice Bílkové, Ph.D., E.MA. za podnětné diskuze a její cené komentáře a podporující přístup během mé práce na této diplomové práci. Také bych rád poděkoval JUDr. Tomáši Minárikovi, vedoucímu oddělení mezinárodních organizací a práva na Národním úřadě pro kybernetickou a informační bezpečnost, za jeho odborné rady od samého počátku mé práce na této diplomové práci. V neposlední řadě bych rád upřímně poděkoval mé rodině a přítelkyni za jejich nesmírnou podporu během celého mého studia.

Contents

Introduction

Cyberspace[1] changes the reality of today's world. It provides us with immense opportunities and benefits, but it also bears risks and security challenges. Activities carried out via cyber means proved efficient for malicious purposes. Many of these activities may have significant impacts on their targets, which include both private entities and States. Moreover, the character of cyberspace enables malicious actors to conduct operations remotely and to obscure their identity. This raises questions on how to protect the rights and interests of the victims of hostile cyber operations and how the responsibility for the operations can be constituted if the source of the operation is unattainable.

On 24 November 2014, an American company, Sony Pictures Entertainment Inc., found itself under a cyber attack after it rejected a request of a hacker group calling itself "Guadians of Peace" to cancel the release of a satirical movie "The Interview" depicting an assassination of the North Korean leader Kim Jong-Un.[2] Consequently, the hacker group released personal information of Sony's employees, such as social security numbers or medical records, and sensitive personal correspondence.[3] Moreover, the attack destroyed Sony's computer systems, which made the company to take its entire network offline.[4] The attack further temporarily disrupted the

1 The glossary of Tallinn Manual 2.0 on the international law applicable to cyber operations defines cyberspace as follows: "*The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks*." In SCHMITT, Michael N et al. Tallinn manual 2.0 on the international law applicable to cyber operations. Second edition. New York, the United States of America: Cambridge University Press, 2017. ISBN 978-1-316-63037-2. Glossary. p. 564. (hereinafter Tallinn Manual 2.0).

2 RUSHE, Dominic, LAUGHLAND, Oliver. Sony cyber attack linked to North Korean government hackers, FBI says. *The Guardian* [online], 19 December 2014. Available from https://www.theguardian.com/us-news/2014/dec/19/north-korea-responsible-sony-hack-us-official.

3 BOORSTIN, Julia. The Sony hack: One year later. *CNBC* [online], 24 November 2015. Available from https://www.cnbc.com/2015/11/24/the-sony-hack-one-year-later.html.

4 Update on Sony Investigation. *FBI.gov* [online], 14 December 2014. Available from https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

company's business activity and allegedly cost Sony tens of millions of dollars.[5] The subsequent FBI (Federal Bureau of Investigation) investigations did not reveal the identity of the responsible hackers. FBI only managed to unveil circumstantial evidence related to the attack.[6] Therefore, the legality of the attribution of the attack to North Korea is questionable.[7] Nevertheless, the investigations disclosed that the North Korean cyber infrastructure[8] was used in the operation.[9] If North Korea was not responsible for the cyber attack, as it claimed,[10] but it knew about the use of its infrastructure in the attack, should it have taken any steps to prevent the attack? And if it did not take any such steps, could it be held responsible for its negligence? More broadly, does the North Korean sovereignty over its cyber infrastructure imply any obligations towards other States? In the following paragraph, I shortly demonstrate how the application of the due diligence principle works on a real-world example. Similar analysis with the same conclusion was also made by Professor Schmitt[11] and other scholars.[12]

The due diligence principle entails an obligation of every State to ensure that its territory is not used for acts contrary to other States' rights. Assuming for the sake of this analysis that North Korea knew about the use of its territory in the attack, it

5 BOORSTIN, Julia. The Sony hack: One year later. *CNBC* [online], 24 November 2015. Available from https://www.cnbc.com/2015/11/24/the-sony-hack-one-year-later.html.

6 Update on Sony Investigation. *FBI.gov* [online], 14 December 2014. Available from https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

7 ZETTER, Kim. Critics Say New Evidence Linking North Korea to the Sony Hack Is Still Flimsy. *Wired* [online], 1 August 2015. Available from https://www.wired.com/2015/01/critics-say-new-north-korea-evidence-sony-still-flimsy/.

8 Cyber infrastructure is an infrastructure composed by "*the communications, storage, and computing devices upon which information systems are built and operate*." See Tallinn Manual 2.0, *supra* note 1. Glossary. p. 564.

9 Update on Sony Investigation. *FBI.gov* [online], 14 December 2014. Available from https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

10 North Korea: Sony hack a righteous deed but we didn't do it. *The Guardian* [online], 7 December 2014. Available from https://www.theguardian.com/world/2014/dec/07/north-korea-sony-hack-a-righteous-deed-but-we-didnt-do-it.

11 SCHMITT, Michael N. International Law and Cyber Attacks: Sony v. North Korea. *Just Security* [online], 17 December 2014. Available from https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/.

12 See, e.g. WALTON, Beatrice A. Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law. *Yale Law Journal*, 2017, vol. 126, no. 5, pp. 1462–1465.

should have taken measures to put an end to the attack violating the United States sovereignty. If it possessed measures to terminate the attack and failed to employ them, it would breach its due diligence obligation. The breach of the due diligence obligation would give rise to North Korean State responsibility under international law. Consequently, the United States could lawfully resort to countermeasures against North Korea. Eventually, the United States announced that it would undertake retaliatory action. Shortly after the announcement, the Internet infrastructure in North Korea experienced two temporal blackouts lasting hours. The United States did not officially acknowledge nor deny that it was behind the outages leaving them in a gray zone. If the blackouts were the retaliatory action promised by the United States, they would be clearly disproportionate – even if the North Korean government itself was the perpetrator of the attack on Sony.

The application of the due diligence principle could provide a legal framework to situations similar to that of the US-North Korean dispute eliminating the avoidance of responsibility and gray-zone operations. Furthermore, its application could bring more mutual respect to States' rights in cyberspace and, consequently, more stability in international relations. While some efforts related to the refinement of the due diligence principle in the cyber context have already been made, much still must be done. This thesis is a contribution to the on-going debate on the adequate application of the due diligence principle and its limits in cyberspace. It aims to comprehensively analyze the due diligence principle and its role and use in the cyber context.

The main goal of this thesis is to examine the adaptability of the due diligence principle to cyberspace and the adequacy of its application therein. In particular, I ascertain whether and how the international community could benefit from the application and whether the application gained any support from the States. Further, I study whether and how the due diligence principle could be applied in the cyber context. Since cyberspace is a very specific environment, I examine what are

the limits of the application of the due diligence priniciple with respect to this specific character.

Although the international law principle of due diligence is mostly known from the famous case of the International Court of Justice (hereinafter ICJ) case *Corfu Channel*, its use in international law has historical origins reaching to the 19th century. Nowadays, its application is reaching to many special international law regimes. Therefore, I briefly introduce the principle of due diligence as a general principle of international law and its historical background in chapter 1 referring to historical cases, subsequent efforts of codification of due diligence in the context of the law of State responsibility, and its use in special international regimes. After this introductory chapter, I will outline the main specific benefits of the application of the due diligence principle in cyberspace in chapter 2.

Chapter 3 reflects the current state of the international mechanisms established within the United Nations, where representatives of States discuss the application of the international law in cyberspace with a special focus on the role of the due diligence principle. In the last section of chapter 3, I introduce and analyze detailed views on the application of the due diligence principle of three States that expressively addressed the principle in their position papers on the application of international law in cyberspace.

Chapter 4 is dedicated to the analysis of how the due diligence principle should be applied in cyberspace. The analysis identifies the basic elements triggering the due diligence obligation and their potential adjustments. Further, some controversial aspects of the application of the due diligence principle are commented on. Lastly, I study legal and practical problems related to the constitution of the breach of the due diligence obligation.

The primary source I use for the analysis in chapter 4 will be Tallinn Manual 2.0, an excellent study on the application of international law to cyber operations. Tallinn

Manual 2.0 is the most authoritative text on the issue produced by academic researchers in cooperation with national legal experts. Where appropriate, I also reflect official State positions on particular issues. It is noteworthy that even though Tallinn Manual 2.0 was published quite recently (in 2017), the mentioned State positions were articulated after the publishment of the Manual. At the time of writing, there is no other comprehensive study on the due diligence principle, which would include both the above-mentioned official positions of States and Tallinn Manual 2.0.

Because the breach of the due diligence obligation, i.e. international obligation, gives rise to State responsibility under international law, the injured States have the right to resort to self-help remedies under the law of State responsibility, which include acts of retorsion and countermeasures. In chapter 5, I overview the legal requirements of these self-help instruments in the light of the specific characteristics of cyberspace.

Ultimately, in chapter 6, I study the preventive feature of due diligence. In international environmental law, the due diligence principle has a relevant preventive feature lying in the principle of prevention. Therefore, I analyze the transferability of this principle into the cyber context. Moreover, I emphasize the influential role posed by certain private entities in relation to the prevention of harm to States and its possible implications.

All of the online sources were accessed between November 2019 and March 2020.

1 The Principle of Due Diligence as a general principle of International Law

The due diligence principle is a well-established and recognized principle of international law deriving from the fundamental international law principle of sovereignty. It was best articulated in the ICJ judgment *Corfu Channel*, where the ICJ held that it is *"every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."*[13] The relation of the due diligence principle to the principle of sovereignty is clear. While States enjoy sovereignty over their territory, they are obligated to protect other States' rights within this territory. As noted in *Island of Palmas case* "*territorial sovereignty [...] involves the exclusive right to display the activities of a State. This right has as corollary a duty: the obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability in peace and in war, together with the rights which each State may claim for its nationals in foreign territory*."[14] However, this obligation to protect is not absolute. Rather than effectively protect other States' rights, States must use their best efforts to do so.

Due diligence is a standard of conduct. The materialization of a result – harm to a State's rights – does not imply non-compliance with the due diligence standard. It is the failure to take available measures to protect other State's rights that imply non-compliance with the standard. The availability of measures always depends on the situation in concern and the capacity of the obliged State. Due diligence is, therefore, adaptable to various contexts and its application is flexible. When a State finds itself in a situation when it has a variety of available measures at disposal, it

13 *Corfu Channel case*, Judgment of 9 April 1949. I.C.J. Reports 1949. p. 22.
14 *Island of Palmas case (United States of America v. Netherlands),* 4 April 1928, Reports of International Arbitral Awards, VOLUME II. p. 839.

can choose which of them it will use.[15] In contrast, it may result that even though a territory of a State was used to cause harm to another State and the territorial State did not take any measures to prevent the harm, the territorial State might still behave in compliance with due diligence standard because no measures available to it could have prevented the harm.

The fundamental element of the due diligence principle is reasonableness.[16] Obligations derived from the due diligence principle should not require States to do more than it should be reasonably expectable from them in given circumstances.[17] Therefore, the reasonableness is the most fundamental factor for the refinement and the application of the due diligence principle, for the development of special due diligence obligations in special international law regimes as well as for the determination of breaches of the due diligence obligations.

1.1 Historical origins of the Application of the Due Diligence Principle

In the context of international law, the due diligence principle was applied for the first time in the late 19th century. The application occurred in an arbitration case known as *Alabama Claims* between the United States of America and Great Britain.[18] In the international arbitration established by the bilateral Treaty of Washington, of the 8th of May 1871, the Brits were found to be in violation of their due diligence obligation by allowing the construction, equipment, and armament of vessels, including a cruiser Alabama, in their ports. Subsequently, these vessels were

15 FRENCH, Duncan (Chair) and Tim STEPHENS (Rapporteur). ILA Study Group on Due Diligence in International Law, Second Report. 2016. p. 9.

16 *Ibid.*

17 Yet, sometimes States go beyond of what is reasonably expectable and provide higher standards of protection of other States' rights. Adhering to such standards is not obligatory under international law, but it significantly contributes to the enhancement of international cybersecurity and mutual trust among States.

18 *Alabama claims of the United States of America v. Great Britain*, Arbitration Award rendered on 14 September 1872 by the tribunal of arbitration established by Article I of the Treaty of Washington of 8 May 1871, Reports of International Arbitral Awards, Volume XXIX, pp.125-134

deployed as warships of the Navy of the Confederate States in American civil war. The United States diplomatic agents knew that the vessels were being constructed in British ports, which should have been neutral, and required the British authorities to put an end to the construction works. Great Britain, at last, did take some measures by ordering the detention of the vessel Alabama but the orders were issued with an extensive delay, which made their execution impossible. To the alleged failure to comply with the due diligence principle, Great Britain stated that "*[i]t is necessary to allege and to prove that there has been a failure to use for the prevention of an act which the government was bound to endeavor to prevent, such care as governments ordinarily employ in their domestic concerns, and may reasonably be expected to exert in matters of international interest and obligation.*"[19] If such a restrictive interpretation were accepted, due diligence standards would be easily limitable by domestic standards and laws.

The arbitrators, however, did not regard this interpretation relevant. Instead, they ruled that "*the government of Her Britannic Majesty cannot justify itself for a failure in due diligence on the plea of insufficiency of the legal means of action which it possessed.*"[20] Hence, Great Britain, as a neutral State, should have acted proportionally to the risks that the construction of warships posed. So even though the arbitrators acknowledged that Great Britain had taken some measures, they qualified them as inadequate to the situation. And being considered insufficient, the measures taken could not release Great Britain from the responsibility. If a similar case got before a judicial organ nowadays, the decision would probably read that Great Britain 'did not take all the feasible measures' available to it at the time. The adequacy of the action that a State should take in order to fulfill its due diligence obligation remains

19 United States Department of State, Office of the Historian. *Case presented on the part of the government of Her Britannic Majesty to the tribunal of arbitration, constituted under Article 1 of the treaty concluded at Washington on the 8th May, 1871, between Her Britannic Majesty and the United States of America,* Papers Relating to the Foreign Relations of the United States, Transmitted to Congress with the Annual Message of the President, December 2, 1872, Part II, Volume I. Document 16, part X.
20 *Alabama claims, supra* note 18. p. 131.

a cornerstone of the due diligence principle so as the non-relevance of domestic law obstacles does. The adequacy required differs on the basis of many factors case-by-case. Therefore, due diligence should always be considered flexibly as it depends on present circumstances.

Since *Alabama Claims*, where the principle of due diligence was applied in the context of the law of neutrality, the principle has found its use in a number of special regimes in public international law. In late 19th Century and early 20th Century, the due diligence principle was mostly applied in arbitration cases related to the protection of aliens in the territory of foreign States. Residing in the territory of foreign States, aliens should have been under the territorial States' protection against criminal acts directed at them or their property. Such criminal acts usually occurred in situations of domestic unrests, occasional violent acts, but also in case of armed conflicts. The obligation of protection also included the duty to duly investigate all those criminal acts.

In *Sambiaggio case,*[21] decided by Italian-Venezuelan mixed commission, an Italian national residing in Venezuela was forced to make advances and hand over his property to revolutionary forces. This case was notable in light of the situation in which the events took place as Venezuela suffered a civil war at that time. For this reason, "*[t]he immediate and most important question presented is as to the liability of the [then] existing government for losses and damages suffered at the hands of revolutionists who failed of success."*[22] To answer this question, the umpire concluded, from the standpoint of general principle, that the Government should not be held responsible for the acts of revolutionists, because revolutionists are not the agents of government. They were beyond governmental control, and no one should be held responsible for the acts of an enemy attempting his life.[23] Nevertheless, the umpire "*accept[ed] the rule that if in any case of reclamation submitted to him it is [sic] alleged*

21 *Sambiaggio Case,* 1903, Reports of International Arbitral Awards, Volume X, pp. 499-525.
22 *Ibid.*, p. 512
23 *Ibid.,* p. 513

and proved that Venezuelan authorities failed to exercise due diligence to prevent damages from being inflicted by revolutionists, that country should be held responsible."[24] And as subsequently noted by the umpire, the mentioned responsibility would be for the acts of the revolutionary forces.[25] Although the view that a State could possibly be indirectly responsible for the acts of its nationals was not rare in the earliest cases,[26] it has been overcome quite soon. One of the first cases where such an approach was rejected was the case *Janes v. Mexico*.[27]

Janes was a United States citizen, superintendent of mines for the El Tigre Mining Company at El Tigre in Mexico. In 1918 he was shot and killed by a Mexican national Pedro Carbajal, a former employee of the mining company. The shooting occurred in the view of many persons in the company's office. Carbajal escaped the place, and even though Mexican authorities were informed about had occurred, they failed to apprehend and punish Carbajal. Consequently, United States alleged Mexico that its authorities "*took no proper steps to apprehend and punish Carbajal; that such efforts as were made were lax and inadequate; that if prompt and immediate action had been taken on one occasion there is reason to believe that the authorities would have been successful.*"[28]

According to United States' opinion presented in *Janes v. Mexico*, "*responsibility rests upon the offending State because by its failure to act it condones and ratifies the wrongful act, thereby making the act its own.*"[29] The arbitrators entitled this concept "indirect responsibility." To acknowledge the application of the "indirect responsibility" would mean that the compensation of the damage caused would be measured in a different manner, which would make it higher. The arbitrators, however, rejected

24 *Ibid.,* p. 524.
25 *Ibid.*
26 DE BRABANDERE, Eric. *Host States' Due Diligence Obligations in International Investment Law*. Syracuse Journal of International Law and Commerce vol. 42, 2015. pp. 319–361. p. 327.
See also *H. G. Venable (U.S.A.) v. United Mexican States,* 8 July 1927, Reports of International Arbitral Awards, Volume IV, pp. 219-261, para. 23.
27 *Laura M. B. Janes et al. (U.S.A.) v. United Mexican States,* 16 November 1925, Reports of International Arbitral Awards, Volume IV, pp. 82-98.
28 *Ibid., p. 83*
29 *Ibid.,* p. 90.

the application of the concept of "indirect responsibility" and instead ruled that governments can be held responsible only for what they commit or omit themselves, not for actions or omissions of their nationals.[30] That did not mean that Mexico avoided responsibility. It was held responsible. But its responsibility was constituted on the basis of the breach of a due diligence obligation, i.e. by the inaction (omission) of its organs to apprehend and punish Carbajal, not by the act of murder. In other words, the murder committed by a Mexican national was not attributable to Mexico. The lack of due diligence of Mexican authorities was.

1.2 Codification efforts in the context of the law of State responsibility

After the essential content of the due diligence principle had taken some shapes, particularly in the light of the arbitration cases concerning the protection of aliens,[31] the topic of due diligence got onto the agenda of the 1930 Hague Conference for the Codification of International Law[32] (hereinafter the Hague Codification Conference) under the issue of "responsibility of states for damage done in their territory to the person or property of foreigners."[33] The protection of aliens was one of the main concerns of the forty-seven States participating in the Hague Codification Conference. Unfortunately, the conference "*failed to adopt even a single recommendation on the subject of State responsibility.*"[34] The failure demonstrated that

30 *Ibid.*, p. 88. It has to be added that, at the time, the arbitrator didn't refuse the indirect responsibiliy absolutely. They retained one exception to the general rule: "*Only in the event of one type of denial of justice, the present one, a State would be liable not for what it committed or omitted itself, but for what an individual did. Such an exception to the general rule is not admissible but for convincing reasons*."

31 See also *The Case of the S.S. "Lotus" (France v. Turkey)*, 7 September 1927, Permanent Court of International Justice, Series A. - No. 10., or *Thomas H. Youmans (U.S.A.) v. United Mexican States*, 23 November 1926, Reports of International Arbitral Awards, Volume IV, pp. 110-117.

32 KOIVUROVA, Timo. Due Diligence. *Max Planck Encyclopedia of Public International Law*. 2010. DOI 10.1093/law:epil/9780199231690/e1034.

33 Preparatory Committee for the Codification Conference. First Report submitted to the Council by the Preparatory Committee for the Codification Conference, *Conference for the Codification of International Law*, Hague, 1930.

34 Codification Division of the Office of Legal Affairs of United Nations. *League of Nations Codification Conference*.

despite States' awareness of the importance of the issue, coming to an agreement on the rules will not be without complications. For the next few decades after the failure of the Hague Codification Conference, the content of the due diligence principle was mostly formed by the State practice and case-law.

As concerns codification efforts related to the due diligence principle posterior to the Hague Conference, eventually, some achievements have been accomplished. Yet, all of them in special international regimes.[35] A general rule of due diligence has not been codified so far. Not that due diligence has not been discussed in the context of State responsibility since the Hague Codification Conference. It has. Even in 1999, only two years before the United Nations International Law Commission (hereinafter ILC) adopted the *Draft Articles on Responsibility of States for Internationally Wrongful Acts*[36] (hereinafter ILC Draft Articles on State Responsibility or Draft Articles), which are generally considered as reflecting customary international law,[37] the ILC was still considering to include due diligence in the Draft Articles.[38]

Nevertheless, James Crawford, the ILC Special Rapporteur on the issue of the State responsibility in 1999 (also in 2001), took a stance that "*defining the precise nature of due diligence could not be done in the context of the draft articles without spending many more years on the topic and, even if the problem were resolved, that would in effect be based on the presumption that any primary rule, or a certain class of primary rules, contained a*

35 FRENCH, Duncan (Chair) and Tim STEPHENS (Rapporteur). ILA Study Group on Due Diligence in International Law, First Report. 2014.

36 International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, New York and Geneva: *Yearbook of the International Law Commission*, vol. II, part 2, 2001 also published as an annex to United Nations General Assembly Resolution 56/83 on Responsibility of States for Internationally Wrongful Acts, A/56/10. 12 December 2001.

37 The United States and China oppose this opinion. See TIKK, Eneken. Will Cyber Consequences Deepen Disagreement on International Law. *Temple International & Comparative Law Journal*, 2018, vol. 32, no. 2. note 8.

38 International Law Commission, Report of the Commission to the General Assembly on the work of its fifty-first session. *Yearbook of the International Law Commission* 1999, Volume II, Part 2, A/CN.4/SER.A/1999/Add.l (Part 2). New York and Geneva, 2003. p. 59.

qualification of due diligence."[39] The due diligence principle was just too complex and too controversial to be included in the final version of the Draft Articles in 2001. As a consequence, the Draft Articles avoided the use of term due diligence completely.[40]

The ILC commentary to the Draft Articles explained the ILC's decision in this regard as follows: "*[t]he articles lay down no general rule… [on] some degree of fault, culpability, negligence or want of due diligence. Such standards vary from one context to another for reasons which essentially relate to the object and purpose of the treaty provision or other rule giving rise to the primary obligation*."[41] And as the Draft Articles focus exclusively on secondary rules,[42] they do not provide any primary rule establishing a due diligence obligation. Therefore, one must look somewhere else to identify primary rules establishing due diligence obligations.

Such rules exist in special international regimes. Besides, there is also a general customary due diligence obligation. I make a short reference to both types of rules in the following two sections. Obligations emanating from these rules are binding and their violation (by omission) together with their attribution to a State constitute two elements of an internationally wrongful act under Article 2 of the Draft Articles. Therefore, the exclusion of the due diligence principle from the Draft Articles cannot be understood as it was meant to impede the constitution of State responsibility on the basis of due diligence.

1.3 General due diligence obligation under international customary law

The due diligence principle has been well reflected and formed by State practice and case-law throughout many years since *Alabama Claims*. Due to its long-time use and

39 *Ibid.*, p. 86.
40 ILA Study Group on Due Diligence, First Report*, supra* note 35. pp. 4-5.
41 ILC Draft Articles on State Responsibility*, supra* note 36. Commentary to Article 2, para. 3.
42 ILA Study Group on Due Diligence, First Report*, supra* note 35. p. 5.

general acceptance, it became applicable under customary international law.[43] From the principle derives a general obligation applicable under international customary law. It is commonly acknowledged that this obligation was best articulated in *Corfu Channel* as "*every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.*"[44]

According to Schmitt, the due diligence principle as a general principle is applicable in particular contexts without further need of the recognition of its applicability. If a State does not accept the applicability in the context of a particular international regime, it has to exclude it by its practice or opinio juris.[45] This ensures that in cyberspace, where the application of international law as a whole is widely accepted,[46] States have a general due diligence obligation (as defined in the *Corfu Channel* judgment) unless they expressively exclude it.[47] This view is also endorsed in Tallinn Manual 2.0 on the international law applicable to cyber operations.[48]

The applicability of the due diligence principle in the cyber context was also recognized by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security in its report to the United Nations General Assembly in 2013. The Group held the view that "*international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT [information and communication*

43 ILA Study Group on Due Diligence, Second Report, *supra* note 15. p. 5.
44 *Corfu Channel, supra* note 13. p. 22.
45 SCHMITT, Michael N. In Defense of Due Diligence in Cyberspace. *The Yale Law Journal Forum*, 2015. p. 73.
46 United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*: Sixty-eighth session, A/68/98, 24 June 2013.
United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Seventieth session*, A/70/174, 22 July 2015.
47 SCHMITT. In Defense of Due Diligence in Cyberspace, *supra* note 45. p. 73.
48 Tallinn manual 2.0, *supra* note 1. Rule 6, paras 3-4.

technology] infrastructure within their territory."[49] This view was endorsed by the same body in 2015.[50]

1.4 Special due diligence obligations applicable in special international law regimes

Some special international law regimes establish their own particular due diligence obligations applicable only within those regimes. Where such obligations exist, their application takes precedence over the general obligation mentioned above.[51] Historically the due diligence principle was applied many times in various contexts. Since the historical cases, where it was applied in the context of international humanitarian law (*Alabama Claims*) and in the context of protection of civilians in foreign territories (*Janes v. Mexico* or *Sambiaggio case*), due diligence has been drawing more and more attention with newly emerging special international regimes. The most apparent example of the current growth of its importance is, without any doubt, international environmental law.[52]

Industrial activities often pose risks for the environment of neighboring States. Such risks are usually predictable and therefore, States have a special due diligence obligation based on the principle of prevention to "*use all the means at its disposal in order to avoid activities which take place in its territory, or in any area under its jurisdiction, causing significant damage to the environment of another State.*"[53] Where there are threats of serious or irreversible damage to the environment, States are obliged to go even further in the protection of other States' environment and apply precautionary approach by taking cost-effective measures to prevent environmental

49 UN GGE 2013 Report, *supra* note 46. para. 20.
50 UN GGE 2015 Report, *supra* note 46. para. 27.
51 ILA Study Group on Due Diligence, Second Report, *supra* note 15. p. 6.
52 Case-law of international environmental law related to the due diligence principle is to be found in the chapter 6.
53 *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Judgment, I.C.J. Reports 2010, pp. 14 - 107. para. 205.

degradation even if there is not full scientific certainty about the threats. The precautionary approach was articulated in the Rio Declaration on Environment and Development.[54]

Besides the international environmental law, the due diligence principle has been applied, for instance, in international law of the sea in relation to the protection of the marine environment.[55] In 2011, the International Tribunal for the Law of the Sea examined the legal nature of States' obligation to ensure that their contractors conducting seabed mining activities comply with their obligations to protect the marine environment. It concluded that this obligation is a special due diligence obligation of conduct.[56]

The researchers of the International Law Association note that the concept of due diligence is also relevant in international human rights law, where it is associated, *inter alia*, with States' obligations to reduce or eliminate violations of individual rights by non-state actors (for instance, within the family or within employment). In some cases, the State's failure to protect the rights of individuals may constitute its responsibility (for the failure to act, not for the violation itself).[57]

Furthermore, due diligence is also widely applied in international investment law, where exist several standards laying down obligations to protect foreign investments and investors. The investment-related due diligence obligations are based on three 'objective standards of treatment' composed of full protection and security standard, international minimum standard, and fair and equitable treatment.[58] The protection States are obliged to provide to the investments and investors under these standards ranges from the physical to legal protection.

54 The United Nations Conference on Environment and Development, *Rio Declaration on Enviroment and Development*. 1992. Principle 15.
55 ILA Study Group on Due Diligence, First Report, *supra* note 35. p. 29.
56 *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, 1 February 2011, Seabed Dispute Chamber of the International Tribunal of the Law of the Sea, Case No. 17. paras. 99 – 120.
57 ILA Study Group on Due Diligence, First Report, *supra* note 35. p. 16.
58 ILA Study Group on Due Diligence, First Report, *supra* note 35. p. 6.

2 Specific benefits of the application of the due diligence principle in cyberspace

The application of a principle requiring more respect and protection to other States' rights might, in general terms, contribute to mutual respect of States and, consequently, to the enhancement of international stability in cyberspace. Besides, there are more specific benefits the application of the due diligence principle might contribute with. An adequate application of the principle might help State victims in dealing with two significant dilemmas international law applicable in peacetime faces in relation to malicious cyber operations. These dilemmas are the attribution problem and the strong influence of malicious non-state actors backed by States.

2.1 Mitigation of the attribution problem

A very enticing argument in favor of the refinement and endorsement of the application of the due diligence principle in cyberspace is that it could help mitigate the most troublesome dilemma of public international law in cyberspace – the attribution problem. The attribution of a cyber operation to a State requires, in short, "*to identify with reasonable certainty the actors and their association with the State*."[59] It is conditioned on a time-consuming, technically demanding process. Even though recent developments indicate that the attribution of cyber operations will likely occur more often,[60] the attribution problem still poses a huge practical obstacle for the application of the law of State responsibility and for the effective and justified resort to self-help remedies. Some highly sophisticated operations,

59 *Kenneth P. Yeager v. The Islamic Republic of Iran*, 2 November 1987, Iran-US Claims Tribunal, Award No. 324-10199-1.

60 MAČÁK, Kubo. Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, 2016, vol. 21, no. 3. p. 410.
See also comments on the attribution of cyber operations against Georgia in the subsection 5.3.1 of this thesis.

such as Stuxnet,[61] are even technically impossible to attribute to a State in a reasonable time, if ever. This enables States to "plausibly deny" their participation in the operations. In contrast, the attribution of conduct constituting a breach of the due diligence obligation is much less demanding.[62] It does not require the identification of the direct perpetrator, nor proof of the association of the perpetrator to the territorial State. Even though the application of the due diligence principle cannot put an end to the culture of plausible deniability, it represents an alternative for the target States incapable of timely identification of the perpetrator.

As concerns the attribution of a cyber operation, the major problem arises from the necessity of the identification of the perpetrator of the cyber operation. To identify a perpetrator and subsequently attribute its conduct to a State requires undertaking an in-depth, time-consuming, and technically complicated investigation resulting in the acquisition of reliable evidence. As the attributing States do not have to publicly expose the evidence proving the attribution, the evaluation of the reliability of the evidence would be up to consideration of each State attributing the operation in concern. However, States should count with the possibility of a subsequent litigation and an assessment of the evidence by a judicial organ.

The ICJ has employed different standards of proof in the proceedings before it and it remains unclear what standard of proof should be met in order to satisfy it.[63] Roscini suggests that the standard of proof likely to be employed in relation to the attribution of the operations qualified as use of force would be "clear and convincing" evidence standard noting that "*a prima facie or preponderance of evidence standard might lead to specious claims and false or erroneous attribution, while a beyond*

61 Stuxnet is a malware that was used to malfunction controlling systems of centrifuges in Iranian nuclear facilities in Natanz in 2010. It is considered to be the first "cyber weapon" in the world.
62 Indeed, State responsibility cannot arise without attribution. Under the law on State responsibility, if a State is alleged of breaching its due diligence obligation, there has to be its behavior constitutes the breach of the obligation attributable to it. The attributed behavior of the State in relation to the due diligence principle would be its omission to act in order to protect other States' rights.
63 H.E. Judge Rosalyn Higgins, President of the International Court of Justice, Speech to the Sixth Committee of the General Assembly, 2 November 2007.

reasonable doubt standard would be unrealistic."[64] The standard of proof may vary according to the seriousness of the operation to be attributed.[65] Nevertheless, the concerns related to the false attribution surround any cyber operation, not only those reaching the threshold of use of force. Cyberspace is an especially predisposed environment to hasty false attributions because it enables the use of identity-obscuring techniques like IP spoofing, onion routing, and the use of botnets. Therefore, the standard of proof must protect States from false attribution, and it should not be lowered only because the attribution is complicated.

The standard of proof related to the alleged breach of the due diligence obligation is equally uncertain. However, what is certain is that the attribution requirements in the case of attribution of lack of diligence are lower than those related to the attribution of malicious cyber operations. The identity of the perpetrator can remain unknown to the target State as well as the existence and degree of the involvement of the non-diligent State in the execution of the operation. What has to be proved in the case of the due diligence is the use of a State territory (or the use of networks and devices under its control), its knowledge of the cyber operation violating the target State's rights and, of course, its omission to take all measures available to it to put an end to the operation.

If a malicious operation were on-going, the knowledge of the territorial State could be easily established and later proved by the notification of the target State to the territorial State of the situation. In response, if the territorial State was not aware of it before receiving the notification, it could either confirm the involvement of its territory in the operation violating the target State's rights and take all feasible measures to put an end to the operation, or ignore the notification, or deny the use of its territory. In the two latter cases, the target State could take countermeasures to

64 ROSCINI, Marco. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. *Texas International Law Journal*, 2015, vol. 50, no. 2-3, p. 252.
65 The Netherlands: International law in cyberspace, *supra* note 108. p. 7.

induce the territorial State to comply with the due diligence obligation[66] if the use of the territorial State's territory in the malicious cyber operation remained conclusive.[67]

In conclusion, the application of the due diligence principle could mitigate the attribution dilemma, particularly in the cases of on-going operations when the identity of the perpetrator is difficult to ascertain, yet it would be clear that the perpetrator operates from a defined State's territory or uses its infrastructure. In such cases, the territorial State has an obligation to take all feasible measures to put an end to the malicious operation. If it failed to do so, the target State could resort to self-help. However, self-help remedies the target State could resort to are limited to countermeasures that must not reach the threshold of threat or use of force. Resorts to self-defense are only allowed after a prior attribution of the cyber operation.

Moreover, the due diligence principle enables target States to overcome the evidentiary hurdle caused by the strict requirement on the identification of perpetrator and its association with the territorial State.[68] Holding the territorial State responsible for, at least, failure of the due diligence obligation is less demanding as it requires evidence "only" on the use of State territory or its infrastructure, its knowledge of the malicious operation, and violation of the target State's rights.

2.2 Denial of safe havens of non-state actors

With the rapid development of information and communication technologies and their omnipresent use, non-state actors gain greater and greater influence in the transnational context. While some private entities are in the front line of the cyber battlefield securing the safety of critical infrastructure of States, cyberspace is,

66 After its prior notification of decision to take countermeasures. See ILC Draft Articles on State Responsibility, *supra* note 36. Article 52.
67 SCHMITT. In Defense of Due Diligence in Cyberspace, *supra* note 45. p. 79.
68 *Ibid.*, p. 80.

sadly, also a perfect environment for the expansion of criminal groups as well as politically motivated non-state actors. Most of cyber operations are not demanding financially, nor personally. This allows non-states actors to conduct hostile operations with massive impact without being dependent on active State sponsorship. Indeed, some malicious cyber activities of non-state actors are actively sponsored by States and carried out under a State's instructions, direction, or control. Accordingly, these activities would be attributable to a State under the law of State responsibility. Consequently, they are covered by the previous section on the attribution problem. In this section, I address the malicious operations of non-state actors passively sponsored by States.

Transforming Byman's concept of passive sponsorship of terrorist groups[69] into the cyber context, Maurer suggests that States passively sponsor non-state actors when they "*simply choose not to prevent the non-state actors' activity, in spite of being aware of the specific operation and capable of stopping it directly or at least warning the victim, presumably because the state perceives that it can benefit from the activity.*"[70] Moreover, the passive sponsorship includes "harboring" of non-state actors in situations when States are not aware of specific malicious cyber operations carried out by non-state actors, but they are aware of the fact that the non-state actors conduct malicious activities from their territories and decide to ignore this fact. By doing so, they provide the non-state actors sanctuary (safe haven).[71] Unlike terrorist groups who attempt to recruit new members, acquire weapons etc., the malicious non-state actors operating in cyberspace need only the sanctuary, and of course, ICT devices.

The due diligence principle cannot provide a solution eliminating all malicious activities of non-state actors in cyberspace. Where non-state actors operate without any knowledge of the territorial State of their activities, or where their operations

69 BYMAN, Daniel. Passive Sponsors of Terrorism. Survival, 2005 – 2006, vol. 47 no. 4. p. 118.
70 MAURER, Tim. Proxies and Cyberspace. *Journal of Conflict and Security Law*, 2016, vol. 21, no. 3. p. 396.
71 *Ibid.*

are out of reach of territorial States, the due diligence principle does not apply. However, it offers a solution for States targeted by cyber operations of non-state actors passively sponsored by territorial States. Under the due diligence principle, if a State is aware of a cyber operation carried out by a non-state actor from its territory that violates other State's rights,[72] it must take all feasible measures to terminate the operation. By failing to do so, it breaches its due diligence obligation. As a consequence of its breach, it commits an internationally wrongful act and can be held responsible for it.[73]

Moreover, the breach of the due diligence obligation permits the target State to respond in compliance with international law, particularly by taking countermeasures. Therefore, the target State could use countermeasures against the territorial State to induce it to put an end to the operations of the non-state actor conducting malicious cyber operations from its territory. In addition, Schmitt advocates that the countermeasures may be targeted directly against the non-state actor, instead of the territorial State in breach of the due diligence obligation.[74] This view is, however, not without controversies.[75] More details on the topic of countermeasures follow in section 6.2.

72 The violation of State's right is one of the elements triggering the due diligence obligation. See the subsection 5.1.3. The element of violation of other States' rights is of special importance in this context. It has to be emphasized that non-state actors that would infringe States' interests causing mere inconveniences to the respective States do not violate States' rights. Also, violations of national laws of the respective States are irrelevant for the sake of the application of the due diligence application in general. Therefore, this special preventive obligation would not relate, for instance, to journalist or human rights defenders based in territories of democratic States that criticize foreign non-democratic governments via online platforms.

73 SCHMITT. In Defense of Due Diligence in Cyberspace, *supra* note 45. p. 79.

74 *Ibid.*

75 JENSEN, Eric T., WATTS Sean. A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer? *Texas Law Review*, 2017, vol. 95. p. 1563.

3 Towards refinement of the due diligence principle in cyberspace

While the applicability of existing norms and principles of international law in cyberspace is generally accepted, how international law should apply in the cyber context remains subject to debate. Academia contributed to the debate, particularly with the excellent work of two International Groups of Experts that shared their views on the application of international law in the cyber context in Tallinn Manual and Tallinn Manual 2.0. The latter includes a very detailed analysis of the application of the due diligence principle in two of its rules (Rule 6 and Rule 7). Although Tallinn Manuals are impressive pieces of work, they do not represent a view of any State, but rather views of independent experts acting solely in their personal capacity.

An essential debate related to the application of international law is taking place within two working groups of the United Nations between representatives of States. These two working groups are subject to sections 4.1 and 4.2. One of the groups was established very recently, and it did not produce any outcome so far. The other one managed to produce valuable reports concerning the general applicability of international law in cyberspace, but they remained somewhat superficial as to the approach to the application of specific norms and principles. Due to the slowness of the processes within the United Nations and the generality of their outcomes, some States decided to publicly deliver their own respective views on the application of specific norms and principles in cyberspace. Some of these declarations even included detailed views on the application of the due diligence principle in cyberspace. These views are introduced in the section 4.3.

3.1 United Nations Group of Governmental Experts

Cybersecurity in the broad sense was on the agenda of the United Nations General Assembly since 1998.[76] After a few years of promoting multilateral cooperation on the issue, the General Assembly on a proposal of the Russian Federation[77] requested Secretary-General to study concepts aimed at strengthening the security of global information and telecommunications systems with the assistance of a group of governmental experts.[78] The group was established in 2004, and it was named United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (hereinafter UN GGE). It comprised representatives of the five permanent members of the Security Council and, in addition, ten more representatives appointed by then Secretary-General on the basis of equitable geographical distribution. Unfortunately, the first UN GGE was not able to produce any consensus report.[79] Another UN GGE was established in 2009. This one was more successful and it eventually did deliver a final report to the General Assembly.[80] However, the report was very superficial and it did not introduce anything noteworthy as concerns due diligence.

The work of the following UN GGE was more productive. In its report issued in 2013, the UN GGE recognized the applicability of principles flowing from sovereignty in the cyber context by stating that "*international norms and principles that flow from*

76 United Nations General Assembly, Resolution 53/70, *Developments in the field of information and telecommunications in the context of international security*, A/RES/53/70. 4 December 1998.
77 United Nations: Recent Developments in the Field of Information and Telecommunications in the Context of International Security. *INCYDER* [online]. Available from https://ccdcoe.org/incyder-articles/united-nations-recent-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security/#footnote_3_2548.
78 United Nations General Assembly, Resolution 58/32, *Developments in the field of information and telecommunications in the context of international security*, A/RES/58/32. 8 December 2003. pp. 2-3.
79 The UN GGE on Cybersecurity: What is the UN's role? *Council on Foreign Relations* [online], 15 April 2015. Available from https://www.cfr.org/blog/un-gge-cybersecurity-what-uns-role.
80 United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/65/201. 30 July 2010.

sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory."[81] This view was endorsed by the same body in 2015.[82] The due diligence principle is one of the principles that flow from sovereignty. Consequently, this applicability recognition relates, inter alia, to the due diligence principle.[83]

Furthermore, the 2013 UN GGE report reflected the due diligence principle in one of the non-binding recommendations the group agreed on, saying that "*States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs.*"[84] In 2015, the following UN GGE broadened the 2013 non-state-actor focused scope of the recommendation by holding that "*States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.*"[85] The wording of the recommendation of 2015 UN GGE was clearly inspired by the *Corfu Channel* dictum.[86] Beyond the scope of the original *Corfu Channel* dictum, the 2015 recommendation includes only a cyber-context feature, which is the inclusion of the ICT elements enabling the commission of internationally wrongful acts.

While the work of the UN GGEs and the two recommendations show goodwill of States in relation to the refinement of due diligence application in cyberspace, the outcome is somewhat weak. The recommendations[87] did not address any specific legal aspects emanating from the nature of cyberspace and their vague wording indicates a hesitant approach of the UN GGEs to the issue.[88] Another attempt to refine due diligence in cyberspace came with the UN GGE active in 2016–2017. This time, however, the UN GGE failed altogether because it was not able to submit a

81 UN GGE 2013 Report, *supra* note 46. para. 20.
82 UN GGE 2015 Report, *supra* note 46. para. 27.
83 Tallinn manual 2.0, *supra* note 1. Rule 6, para 3.
84 UN GGE 2013 Report, *supra* note 46. para. 23.
85 UN GGE 2015 Report, *supra* note 46. paras. 13 (c), 28 (e).
86 See *Corfu Channel, supra* note 13. p. 22. Note that instead of using formulation *acts contrary to the rights of other States*, the UN GGE used the expression *internationally wrongful acts* employing the terminology of the Draft Articles.
87 UN GGE 2015 Report, *supra* note 46. para. 13.
88 SCHMITT. In Defense of Due Diligence in Cyberspace, *supra* note 45. p. 73.

final report to the General Assembly due to disagreements on some controversial issues between the members.[89] The eventual failure is particularly regrettable, considering the progress that had been made before the process failed. For instance, in relation to due diligence, the States agreed on the content of the knowledge requirement. The UN GGE also sought to take action against non-state actors using States' infrastructure for malicious purposes.[90]

After the failure of UN GGE in 2017, some commentators thought that the UN GGE process came to its end, and the international community had to find an alternative platform to discuss the international norms applicable to cyberspace.[91] This was only partially true. The United States did not want to give up on the UN GGE mechanism. One year later, it proposed to the General Assembly to set up another UN GGE. On 8 November 2018, the United Nations First Committee (Disarmament and International Security) of the General Assembly adopted the resolution A/C.1/73/L.37 sponsored by the United States. On the basis of this resolution, a new UN GGE was created in 2019. Unlike the previous expert groups, this one seeks to collaborate with relevant regional international organizations and also hold open-ended informal consultative meetings with all Member States of the United Nations willing to share their views. The process now underway, and the final session of this UN GGE is scheduled on May 2021. The question is whether this group will be able to agree on a final report enhancing the acceptable application of international norms in cyberspace like its predecessors did in 2013 and 2015.

89 SUKUMAR, Arun M. The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?. *The Lawfare Institute* [online], 4 July 2017. Available from https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.
90 *Ibid.*
91 *Ibid.*

3.2 United Nations Open-Ended Working Group

The US-sponsored resolution was not the only important cyber-related resolution the UN First Committee of the General Assembly adopted on 8 November 2018.[92] There was one more tabled by the Russian Federation. The second resolution (A/C.1/73/L.27.Rev.1)[93] aimed to convene an open-ended group working group (hereinafter OEWG) acting on a consensus basis "to further develop the rules, norms and principles of responsible behavior of States."[94] By "further" it is referred to the fact that the work of OEWG should build upon the recommendations of the reports of the UN GGEs. Nonetheless, some State delegations that voted against the resolution alleged that the UN GGE reports reflected in the resolution were "cherry-picked"[95] and the resolution includes selected excerpts from reports that distort their meaning.[96] As regards specifically the wording of the due diligence principle, it was left in the original wording of the 2015 UN GGE recommendation.

According to the resolution, the OEWG should be more democratic, inclusive and transparent as it comprises of all the Member State of the United Nations[97] and it provides the possibility of holding consultative meetings with interested parties, namely business, non-governmental organizations and academia, to share views on the issues within the group's mandate.[98] This inclusive and transparent policy has

92 GUPTA, Arvind. A Tale of two UN Resolutions on Cyber-security. *Vivekananda International Foundation* [online]. 29 April 2019. Available from https://www.vifindia.org/2019/april/24/a-tale-of-two-un-resolutions-on-cyber-security.

93 Available online from https://undocs.org/A/C.1/73/L.27/Rev.1.

94 The United Nations First Committee (Disarmament and International Security) of the General Assembly, *Developments in the field of information and telecommunications in the context of international security*, A/C.1/73/L.27/Rev.1. 29 October 2018. para. 5.

95 Statement of representative of Canada in First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct. *United Nations Meetings Coverage* [online]. Available from https://www.un.org/press/en/2018/gadis3619.doc.htm.

96 *Ibid.*

97 In the First Committee meeting, the Russian representative introduced the Resolution A/C.1/73/L.27.Rev.1 by saying that "[t]he practice of some 'club agreements' should be sent into the annals of history" referring to the UN GGE process.

98 The United Nations First Committee (Disarmament and International Security) of the General Assembly, *Developments in the field of information and telecommunications in the context of international*

already been turned into action. From 2 to 4 December 2019, an intersessional meeting of OEWG with the participation of industry, non-governmental organizations and academia was held.[99]

The democratic character noticeably lies in the participation of all the Member States of the United Nations. While the mere fact that all States are welcomed to participate in the OEWG is commendable, it raises doubts about the capacity of the OEWG to come to an agreement on more than merely superficial issues. The outcome should be known in July 2020 (and if successful, it will be submitted to the General Assembly in its 75th session in September 2020). Nevertheless, it may happen that the whole process will be prolonged due to the situation related to the spread of Coronavirus Disease (COVID-19), which is particularly worrisome in New York, where the meetings of the OEWG take place.

Not only the difficulty of reaching consensus due to the broad participation States raises concerns about the OEWG mechanism. Some States consider the setting up of the Russian-proposed working group with a similar mandate to that of simultaneously existing UN GGE as an attempt to promote extensive State control over ICT infrastructure enabling mass surveillance and censorship.[100] For a long time, Russia, together with other like-minded States, is trying to promote such an approach towards domestic ICT infrastructures. These efforts are repeatedly criticized because of the negative impacts an extensive State control over ICTs could have on human rights and the freedom of the Internet.

---

security, A/C.1/73/L.27/Rev.1. 29 October 2018. para. 5.

99 Informal intersessional consultative meeting of the OEWG with industry, non-governmental organizations and academia (2-4 December 2019). *United Nations Office for Disarmament Affairs* [online]. Available from https://www.un.org/disarmament/oewg-informal-multi-stakeholder-meeting-2-4-december-2019/.

100 DE TOMAS COLATIN, S. A surprising turn of events: UN creates two working groups on cyberspace. *The NATO Cooperative Cyber Defence Centre of Excellence* [online], 11 March 2019. Available from https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/.

From the strict due diligence point of view, increased monitoring of an ICT infrastructure implies a gathering of more information about ongoing operations in the infrastructure. More timely information enables States to enhance their due diligence practice.[101] According to the resolution that convened the OEWG, the enhancement of due diligence is a priority task for the OEWG.[102] The diligent behavior of States firmly controlling their infrastructures towards other States would signify more international security. That is the theoretical pro-due-diligence-positioned way to read the demands for strengthening the domestic control. More realistically, as noted above, Russia and its supporters aim to advance their surveillance and censorship capacity. Diligent behavior with the objective of protecting other States probably was not their primary aspiration.

The resolution that convened the OEWG set as the primary goal of the OEWG work the development of international rules, norms and principles of responsible State behavior elaborated in the UN GGE recommendations, including due diligence, and the ways for their implementation. As stated in the resolution, reaching that goal may also be achieved by the introduction of changes to them. While the adoption of the setting up of the OEWG was accompanied by skeptical voices, it will be interesting to observe where the OEWG process, along with the UN GGE process, will lead to.

So far, two of the three substantive sessions took place. Interestingly, during the second substantive session held in February 2020, seven States delivered statements addressing the issue of how international law applies to the use of information and communications technologies by States.[103] Three of them also addressed specifically

101 Insufficient of control over cyber infrastructures is often used as an excuse for non-application of due diligence.

102 The United Nations First Committee (Disarmament and International Security) of the General Assembly, Developments in the field of information and telecommunications in the context of international security, A/C.1/73/L.27/Rev.1. 29 October 2018. para 5.

103 The statements are available from https://papersmart.unmeetings.org/ga/oewg-on-icts/2020-2nd-substantive-session/agenda/5/5d/.

the due diligence principle. Brazil endorsed the application of the principle in cyberspace and furthermore emphasized that the principle should be applied flexibly, respecting different national capabilities. Finland also expressed its support, noting that the principle of due diligence is "*particularly pertinent in the cyber environment*."

Lastly, the delegation of Argentina stressed that the application of the principle of due diligence should be adjusted to the special characteristics of cyberspace. Interestingly, it suggested that the application of the due diligence principle should consist exclusively of the assistance of territorial States provided to target States whose critical infrastructures were targeted by malicious cyber operations. The assistance would follow after a previous request of assistance of the target State and would be limited to the only purpose, which would be the termination of the operations.

3.3 States' declarations on the due diligence principle application

Regardless of the processes within the United Nations, some States decided to step up and express their opinions on how international law should apply in cyberspace from their national standpoints. This could potentially lead to an acceleration of processes within the international mechanisms mentioned above, or potentially to their substitution. Where a broad agreement on particular issues would exist, even customary rules could arise – clearly, only with sufficient support in State practice.

As of March 2020, seven States have made their declarations on the application of international law in the context of cyberspace. The States who made their declarations on the application of international law in cyberspace are Australia,[104]

104 Australia's International Cyber Engagement Strategy. 2017. ISBN 978-1-74322-412-0.

Estonia,[105] France,[106] Germany,[107] the Netherlands,[108] United Kingdom,[109] and the United States.[110] All the declarations are relatively recent. With two exceptions (Germany and the United States), all of them were delivered after the failure of the UN GGE process in 2017. Doubtlessly, more declarations will follow soon. Finland already announced that it is working on its own articulation on the topic.[111] In three of the seven already articulated declarations, comprehensive reflections on the due diligence applications are to be found. As Finland already addressed the topic of due diligence, calling it "particularly pertinent in the cyber environment,"[112] it is very likely that its reflection will follow. In addition, one declaration, the Estonian, does not include a detailed view on the due diligence principle, but it endorses its application by holding that "*states have to make reasonable efforts to ensure that their territory is not used to adversely affect the rights of other states*."[113]

First State, which expressed its detailed view on the due diligence principle in cyberspace, was Australia in 2017. In its opinion:

105 President of the Republic at the opening of CyCon 2019. *President of Estonia* [online], 29 May 2019. Available from https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html.
106 Ministère des Armées. International law applied to operations in cyberspace. 2019.
107 "Cyber Security as a Dimension of Security Policy". Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London. *Federal Foreign Office* [online], 18 May 2015. Available from https://www.auswaertiges-amt.de/en/newsroom/news/150518-ca-b-chatham-house/271832.
108 Government of the Kingdom of the Netherlands, 2019, Appendix: International law in cyberspace to the letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace. 26 September 2019.
109 United Kingdom Attorney General's Office. *Cyber and International Law in the 21st Century* [online]. 23 May 2018. Available from https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
110 EGAN, Brian J. International Law and Stability in Cyberspace. Berkeley Law, 10 November 2016.
111 Statementby Ambassador Janne Taalas at the second session of the open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, 10 and 11 February 2020.
112 *Ibid.*
113 President of the Republic at the opening of CyCon 2019. *President of Estonia* [online], 29 May 2019. Available from https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html.

> To the extent that a state enjoys the right to exercise sovereignty over objects and activities within its territory, it necessarily shoulders corresponding responsibilities to ensure those objects and activities are not used to harm other states. In this context, we note it may not be reasonable to expect (or even possible for) a state to prevent all malicious use of ICT infrastructure located within its territory. However, in Australia's view, if a state is aware of an internationally wrongful act originating from or routed through its territory, and it has the ability to put an end to the harmful activity, that state should take reasonable steps to do so consistent with international law.[114]

There are two crucial aspects Australia expressed in its view. First, that the prevention of all the malicious use of ICT infrastructure located in a State's territory would be unreasonable to expect (if not directly impossible). And second, when acknowledging that a State should take reasonable steps to put an end to the ongoing harmful activity that it is aware of, it said that the internationally wrongful act that is underway can either originate from the State's territory or can be routed through it.

France was the second State that made a commentary of the due diligence principle. It came in September 2019 in a very comprehensive document called "International Law Applied to Operations in Cyberspace" published by the French Ministry of the Armies (Ministry of Defense).

> France exercises its sovereignty over the information systems located on its territory. In compliance with the due diligence requirement, it ensures that its territory is not used for internationally wrongful acts using ICTs. This is a customary obligation for States, which must (i) use cyberspace in compliance with international law, and in particular not use proxies to commit acts which, using ICTs, infringe the rights of other States, and (ii) ensure that their territory is not used for such purposes, including by non-state actors.[115]

114 Australia's International Cyber Engagement Strategy, *supra* note 104. p. 91.
115 France: International law applied to operations in cyberspace, *supra* note 106. p. 6.

> In accordance with the due diligence principle, "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs", including acts that infringe the territorial integrity or sovereignty of another State. In addition, States must ensure that non-state actors do not use their territory to carry on such activities, and not use proxies to commit internationally wrongful acts using ICTs.[116]

In the first cited paragraph, France expressed its strong support for the application of the due diligence principle in cyberspace and, in fact, identified cyber due diligence as a customary international obligation. In the second cited paragraph, it specified the content of this obligation in its view by quoting the 2015 UN GGE recommendation and adding that the internationally wrongful acts that should not be allowed to be carried out include infringement of the territorial integrity or sovereignty of other State. It is noteworthy that, in the French perspective, the act that constitutes a breach of sovereignty is "*[a]ny cyberattack against French digital systems or any effects produced on French territory by digital means by a State organ, a person or an entity exercising elements of governmental authority or by a person or persons acting on the instructions of or under the direction or control of a State*."[117] The French understanding of due diligence in cyberspace is, therefore, remarkably extensive.

So far, the last declaration addressing the application of the due diligence principle in cyberspace was delivered by the Netherlands, also in September 2019. The Dutch government first emphasized that it regards "*the principle [of due diligence] as an obligation in its own right, the violation of which may constitute an internationally wrongful act.*"[118] Then it introduced of what elements the due diligence principle in the context of cyberspace encompasses in its view and set forth an example of the application of the principle.

---

116 *Ibid.,* p. 10.
117 *Ibid.,* p. 7.
118 The Netherlands: International law in cyberspace, *supra* note 108. p. 4.

> In the context of cyberspace, the due diligence principle requires that states take action in respect of cyber activities:
>
> - carried out by persons in their territory or where use is made of items or networks that are in their territory or which they otherwise control;
> - that violate a right of another state; and
> - whose existence they are, or should be, aware of.
>
> To this end a state must take measures which, in the given circumstances, may be expected of a state acting in a reasonable manner. It is not relevant whether the cyber activity in question is carried out by a state or non-state actor, or where this actor is located. If, for example, a cyberattack is carried out against the Netherlands using servers in another country, the Netherlands may, on the basis of the due diligence principle, ask the other country to shut down the servers, regardless of whether or not it has been established that a state is responsible for the cyberattack.
>
> It is generally accepted that the due diligence principle applies only if the state whose right or rights have been violated suffers sufficiently serious adverse consequences. The precise threshold depends on the specific circumstances of the case. It is clear, however, that such adverse consequences do not necessarily have to include physical damage.[119]

The Netherlands' declaration is definitely the most precise one. In contrast to the perspectives of Australia and France, the Netherlands broadened the scope of the application of the due diligence principle from the infrastructures located in a State's territory to the items and networks which it *otherwise control* outside its territory. Besides, the Netherlands was the only State which made a reference to the constructive knowledge standard by holding that the due diligence attaches not only when a State is actually aware of the existence of the malicious cyber activity, but also when it should be aware of it.

119 *Ibid.,* pp. 4–5.

The declarations were, to a great extent, focused on the determination of elements that trigger the due diligence obligation. After making their comparison, it seems that there are three elements all States included in their declarations. The first one is the involvement of State territory.[120] The second element is the violation of a State's rights. And the last one is actual knowledge. That means due diligence is triggered when a State becomes aware of malicious activity originating from its territory and violating other State's rights.[121]

Unfortunately, the overlap of the articulations found in the declarations suffices only to cover the general customary due diligence obligation laid down in *Corfu Channel*, and its slightly modified version in the 2015 UN GGE recommendation. While there were not any disagreements on other aspects, many of them were left uncommented. As a consequence, beyond the elemental due diligence articulations (Corfu Channel and 2015 UN GGE recommendation), the common standpoint of the three States does not capture any cyber-specific issues the due diligence principle comes within the context of cyberspace, leaving all the controversies unresolved.

120 Moreover, Australia and the Netherlands broadened the scope of the application also to the infrastructure located outside of a State territory.
121 The Netherlands included also the constructive knowledge to its articulation.

4 The Application of Due Diligence Principle in the cyber context

Being far from perfectly refined in the cyber context, the due diligence principle has been repeatedly recognized as applicable in cyberspace. Therefore, I now shift from overviewing of the interstate debates and position forming to a more practical issue – the analysis of the application of the due diligence principle. It is not my intention to provide exhausting application guidelines. It is not even possible to do that because the application of the due diligence principle is too circumstances-dependent, and cyberspace is developing too rapidly. Rather I will focus on the elements triggering the due diligence obligation and their possible adjustments, then on the content of the due diligence obligation when it gets triggered on the basis of the triggering elements and ultimately on the constitution of the breach of the due diligence obligation.

4.1 Elements triggering the due diligence obligation

Building upon the articulation of the due diligence principle in the 2015 UN GGE report,[122] as well as all to-date available declarations of States on the application of the due diligence principle[123] and the general articulation the due diligence principle in the case-law,[124] I identified three elements triggering the due diligence obligation: (1) use of the territorial State's territory or its cyber infrastructure in the malicious operation, (2) knowledge the territorial State has of a cyber operation that is supposed to be stopped (knowledge requirement), and (3) violation of other State's rights. While it is indisputable that these elements trigger the due diligence obligation, there are some important nuances in their content that deserve to be

122 See section 4.1.
123 See section 4.3.
124 See chapter 1.

commented on. Moreover, the application of the due diligence principle might be extended as well as restricted by certain adjustments to the three elements. Each of the three elements might be adjusted by one corresponding potential adjustment. Which of the adjustments will be used in practice, and how, depends on the further refinement efforts relating to the due diligence principle and State practice.

4.1.1 Use of the State territory

The involvement of a State territory is a key prerequisite of the due diligence obligation because it is the State territory where the State exercises its sovereignty, where its cyber infrastructure is located and where it is obligated to ensure the protection of other States' rights under the due diligence principle. In short, States are obligated to ensure that their territory is not used in cyber operations violating other States' rights. The territorial element is inherently connected to the due diligence principle since the very beginning of its application in *Alabama Claims*. Without any doubt, the involvement of a State territory is a fundamental indicator that the State in concern might owe the due diligence obligation. Nonetheless, the involvement of the State territory could not be the only indicator in this sense.

Extraterritoriality

The Netherlands proposed in its declaration to extend the application of the obligation to the items and networks not located on a State territory that are, nonetheless, under the State control.[125] The International Group of Experts is of the same view, adding that the due diligence obligation should apply extraterritorially in two cases. First, when a State is in control of a territory but does not exercise sovereignty over it, which would be, for instance, the case of an annexation of a territory or an occupation.[126] Second, when a State controls government cyber

125 The Netherlands: International law in cyberspace, *supra* note 108. p. 4.
126 Tallinn manual 2.0, *supra* note 1. Rule 6, para 9.

infrastructure located on a territory of another sovereign State, such as cyber infrastructures in diplomatic premises or military installations.[127]

4.1.2 Knowledge requirement

The due diligence obligation is triggered when a State has an actual knowledge of malicious use of its cyber infrastructure. In other words, once a State learns of a cyber operation causing violation of another State's rights, the due diligence obligation triggers. This actual knowledge requirement is generally recognized as a basic condition for the attachment of the obligation by States,[128] as well as the 2015 UN GGE.[129] While the substance of the requirement is not controversial, proving that the obliged State gained knowledge of an operation may cause trouble. The relevant evidence related to the actual knowledge is usually administered by the obliged States, which makes it inaccessible for anyone else except the obliged State itself.[130] The only occasion when the evidentiary situation would be relatively favorable for the target State would occur if the target State notified the obliged State of the fact that its infrastructure was being used in an operation causing significant damage to the target State.[131] The obliged State's claims that it was unaware of the operation would be pointless because the target State could easily prove the opposite.

The knowledge element is based on the idea that holding States responsible for not putting an end to operations they could not have any knowledge of would be unreasonable. Nevertheless, it should not be allowed to let the States be ignorant to misuses of their cyber infrastructures resulting in significant harm to other States. Therefore, the knowledge requirement should also be satisfied when the

127 *Ibid.*, Rule 6, paras 10–12.
128 See section 4.3.
129 See section 4.1.
130 COUZIGOU, Irène. Securing cyber space: the obligation of States to prevent harmful international cyber operations, *International Review of Law, Computers & Technology*, vol. 32, no. 1, 2018. DOI: 10.1080/13600869.2018.1417763. p. 42.
LIU, Ian Y. State Responsibility and Cyberattacks: Defining Due Diligence Obligations. *The Indonesian Journal of International & Comparative Law*, 2017. ISSN 2338-7602. pp. 233 – 234.
131 *Cf.* Liu, *supra* note 130. p. 234–235.

circumstances of the case leave no doubt that the State should have known that its cyber infrastructure was used to cause violation of other State's rights. Such construction of State knowledge would be possible by the application of the constructive knowledge concept commented below.

Constructive knowledge

To avoid the ignorance of States related to misuses of their cyber infrastructures and, more importantly, to suppress the culture of plausible deniability, the due diligence obligation should attach also when States "should have known" of malicious use of their cyber infrastructure. In this case, however, the due diligence obligation would not be "triggered", because it would attach retrospectively. The use of this concept known as 'constructive knowledge' is supported by the IGE, which suggests that "*if the factual circumstances are such that a State in the normal course of events would have become aware of said use, it is appropriate to constructively attribute knowledge to the State*."[132] Liu also endorsed this view,[133] and so did the Netherlands.[134] Other States did introduce neither positive nor negative views in this regard.

The determination if a State should objectively have known of a certain cyber operation would have to be conducted by a judicial organ case-by-case. As many different factors may come into consideration, holding a State responsible for a breach of the due diligence obligation based on constructive knowledge requires an adequately profound assessment of the evidence. The IGE notes that if attackers used publicly known malware or exploited known vulnerabilities, the constructive knowledge would be established more easily.[135] The same applies in case of involvement of State's governmental infrastructure in the harmful operation.[136] Other scholars suggest that constructive knowledge is likely to be constructed when

132 Tallin Manual 2.0, *supra* note 1. Rule 6, para 39.
133 Liu, *supra* note 130. pp.197, 232, 235 – 241.
134 The Netherlands: International law in cyberspace, *supra* note 108. p. 4.
135 Tallin Manual 2.0, *supra* note 1. Rule 6, para 40.
136 *Ibid.*

the cyber operation is traceable to a single State,[137] "*when the State intensively guards its cyber infrastructure, when the cyber operation involves a cyber activity that is generally always detected such as a Distributed Denial of Service attack that significantly increases bandwidth usage compared to normal usage, or when the State's cyber infrastructure has already been exploited for the purpose of conducting a series of similar offensive cyber operations.*"[138]

Some scholars even advocate a reverse *presumptio juris* in the case of the involvement of the governmental infrastructure.[139] According to their view, the States alleged of breaching the due diligence obligation would have to prove that they did not pose the presumed constructive knowledge. However, this view is not supported by the ICJ case-law.[140] If the constructive knowledge concept was employed in cyberspace, it should be applied rather restrictively.[141] For instance, the mere indication of involvement of State's governmental infrastructure combined with high-intensity State control over it does not unequivocally imply that the State should have known of the use of its infrastructure.[142] It could be possible that governmental infrastructure was compromised by previously unknown malware and used to cause significant harm to other State without any knowledge of the territorial State and the circumstances of the case would be such that it could not be reasonably expectable that the territorial State should have known of the malicious use of its infrastructure. Moreover, it should be remembered that different levels of technological capabilities different States possess also play a significant role in assessing what is reasonably expectable that a State should have been aware of in given circumstances.

137 Liu, *supra* note 130. p. 237.
138 Couzigou, *supra* note 130. p. 42.
139 *Ibid.*, p. 43.
Liu, *supra* note 130. p. 237.
140 *Corfu Channel, supra* note 13. p. 18.
ROSCINI, Marco. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. *Texas International Law Journal*, 2015, vol. 50, no. 2-3, pp. 245 – 248.
141 Liu, *supra* note 130. pp. 239 – 240.
142 *Corfu Channel, supra* note 13. p. 18.

In the *Corfu Channel* case, the ICJ acknowledged that even though the exclusive control of State over its territory can, by itself, neither establish responsibility nor shift the burden of proof, the harmed States might face evidentiary hurdle to gather direct proofs of facts giving rise to responsibility because of the exclusivity of the territorial State's control. Therefore, the harmed State "*should be allowed a more liberal recourse to inferences of fact and circumstantial evidence*"[143] leaving no room for reasonable doubt.[144] Accordingly, States could present indirect evidence, for instance, in the case when a State's infrastructure has been repeatedly used by a single attacker (or group of attackers) in operations with similar *modus operandi* against a certain State and there is an indication that it will be used for such purposes again. If the attacker caused significant harm to the target State by using the territorial State's cyber infrastructure employing the same *modus operandi* as it did on previous occasions, constructive knowledge of the territorial State could be established on the basis of evidence presented by the target State related to the repeatedly used *modus operandi* demonstrating the connection between malicious cyber operations and the territorial State's cyber infrastructure.

The application of constructive knowledge doubtlessly increases the standard of due diligence in cyberspace. It precludes States from being ignorant to what is happening in their cyber infrastructures, and also from backing up hacker groups repeatedly causing significant harm to other States. The basic criterion for the assessment of constructive knowledge is meeting reasonable expectations in the normal course of events. Logically, the question of what is reasonably expectable that States should normally do in order to meet the criterion arises. The IGE opposed the hypothesis that States should be obliged to take preventive measures for this purpose, in particular, to monitor their networks or take similar steps alerting authorities of malicious use of cyber infrastructure. Instead, it concluded that "*if the factual circumstances are such that a similarly situated and equipped State in the normal*

143 *Ibid.*
144 *Ibid.*

course of events would have discovered the use of the cyber infrastructure in question, it is appropriate to conclude that the knowledge criterion is satisfied."[145] Even though the vagueness of the IGE formulation is not fully satisfactory, it should be remembered that due diligence is a flexible standard and presuming what States should have known is somewhat dangerous. From this point of view, the vagueness of the IGE conclusion is justified.

4.1.3 Violation of State's rights

The due diligence obligation may be triggered only when State's rights are violated.[146] This triggering element ensures that States do not bear an obligation to take measures to terminate operations that cause only minor disruptions or mere inconvenience to the target States.[147] Consequently, the due diligence obligation relates only to situations when a certain threshold of seriousness was reached. While this basic premise is undisputable, the determination of the threshold of seriousness is not without controversies.

First of all, the question of which rights of States can be violated in cyberspace is a subject of a deep and dividing discussion between States. Specifically, the issue of whether the prohibition of violation of sovereignty is a rule on its own causes troubles. United Kingdom argues that there is no specific rule prohibiting violation of territorial sovereignty, stating that it is not possible to "*extrapolate from the general principle [of sovereignty] a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention*."[148] Consequently, sovereignty cannot be a value protected by the due diligence principle in the UK view and the violation of sovereignty cannot constitute a violation of the due diligence obligation. As of early

145 Tallinn Manual 2.0, *supra* note 1. Rule 6, para 42.
146 States' rights might be violated also by operations targeting non-state actors if their right are violated. See Tallinn Manual 2.0, *supra* note 1. Rule 6, para. 36.
147 Tallinn Manual 2.0, *supra* note 1. Rule 6, para. 26.
148 United Kingdom Attorney General's Office. Cyber and International Law in the 21st Century [online]. 23 May 2018. Available from https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

2020, United Kingdom is the only State advocating this view.[149] There are some indications that the United States may also adopt the same view.[150] Nevertheless, the United States position is yet to be clarified.

France has quite the opposite opinion on sovereignty. It argues that *"[a]ny cyberattack against French digital systems or any effects produced on French territory by digital means by a State organ, a person or an entity exercising elements of governmental authority or by a person or persons acting on the instructions of or under the direction or control of a State constitutes a breach of sovereignty*."[151] This is the broadest understanding of the breach of sovereignty possible. Therefore, the gravity of the breach has to be further evaluated case-by-case and after the evaluation of the gravity of the cyber operation, the State decides how to respond to the breach appropriately. In the French view, from the principle of sovereignty does derive a right on its own. Similarly to France, the Netherlands "*believes that respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act*."[152] Moreover, the Netherlands referred to the ICJ opinion expressed in the *Nicaragua* case that there is an "*obligation under customary international law not to violate the sovereignty of another State.*"[153] Also Germany shares the same view.[154] The authors of Tallinn Manual 2.0 unanimously agreed on the same opinion that the Netherlands, France and

149 ROGUSKI, Przemysław. Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace. *Just Security* [online]. 6 March 2020. Available from https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/.

150 DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, *United States Department of Defense* [online], 2 March 2020. Available from https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

151 France: International law applied to operations in cyberspace, *supra* note 106. p. 7.

152 The Netherlands: International law in cyberspace, *supra* note 108. p. 2.

153 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),* Judgment, I.C.J. Reports 1986. paras. 15, 252, 292.

154 "Cyber Security as a Dimension of Security Policy". Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London. *Federal Foreign Office* [online]. 18 May 2015. Available from https://www.auswaertiges-amt.de/en/newsroom/news/150518-ca-b-chatham-house/271832.

Germany have in relation to the prohibition of violation as a standalone rule of international law.[155]

Whereas the United Kingdom advocates the opinion that there is no rule prohibiting violation of sovereignty, it recently condemned Russia for undermining Georgia's sovereignty by attributing a large-scale disruptive cyber attack on Georgia that on 28 October 2019 left some of governmental and national media services inoperable for some time[156] to GRU – Russia's military intelligence service. It further suggested that this Russian behavior is disrespectful of international law.[157] That contradicts the UK's resistant position related to sovereignty as a standalone rule unless the UK would qualify it as prohibited intervention.

Roguski argued that the Georgian case revealed the weakness of the UK's position of "sovereignty as principle only".[158] He stressed that if the Russian attacks on Georgia would not be qualified as a breach of the "sovereignty rule," there would not be any other rule possibly qualified as violated, and Russia could not bear any responsibility under international law because the attack would fall below the threshold of use of force as well as prohibited intervention.[159] That would make the attack lawful (unless the UK would actually qualify it as prohibited intervention). Moreover, Russia would not breach its due diligence obligation even if it knew that the attack was underway, who was the perpetrator,[160] and still did not even try to take any measures to put an end to it.

---

155 Tallinn manual 2.0 , *supra* note 1. Rule 4.
156 Georgia hit by massive cyber-attack. *BBC* [online]. 28 October 2019. Available from https://www.bbc.com/news/technology-50207192.
157 UK condemns Russia's GRU over Georgia cyber-attacks. *GOV.UK* [online], 20 February 2020. Available from https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.
158 ROGUSKI, Przemysław. Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace. *Just Security* [online]. 6 March 2020. Available from https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/.
159 *Ibid.*
160 Without distinction of the involvement of GRU in the attack.

On the other end of the "sovereignty as a rule" discussion is the French view considering any cyber attack or any effects produced on French territory by digital means attributable to a State as a breach of sovereignty – a violation of State's right. Accordingly, any cyber attack or effects by digital means would trigger the due diligence obligation. That is certainly not desirable. If the French view of the threshold of violation of sovereignty were applied, there would have to be another additional threshold for the determination of the attachment of the due diligence obligation. France did not introduce any additional threshold in this regard. Unlike the IGE and the Netherlands. See below.

Advocating the "sovereignty as a rule", Germany did not address the threshold for violation of sovereignty. The Netherlands noted that due to the alternations and uncertainties the cyberspace brings to the concepts of territoriality and physical tangibility the "*precise boundaries of what is and is not permissible have yet to fully crystallise*."[161] The authors of Tallinn Manual 2.0 offered some guiding criteria that could be use when determining the threshold of violation of sovereignty, but their views were divided when they assessed the criteria, so they ended up with the same unsatisfactory result like the Netherlands noting that the threshold needs to be clarified by the State practice.[162] The practice seems to be evolving already, triggered by the collective attribution of the above-mentioned 2019 cyber attack on Georgia. Besides United Kingdom, the United States[163] and many European States[164] also

161 The Netherlands: International law in cyberspace, *supra* note 108. p. 2.
162 Tallinn Manual 2.0, *supra* note 1. Rule 4.
163 The United States Condemns Russian Cyber Attack Against the Country of Georgia. U.S. Department of State [online], 20 February 2020. Available from https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/.
164 Statement of the Polish MFA on cyberattacks against Georgia. *Ministry of Foreign Affairs of Republic of Poland* [online], 20 February 2020. Available from https://www.gov.pl/web/diplomacy/statement-of-the-polish-mfa-on-cyberattacks-against-georgia. The Netherlands considers Russia's GRU responsible for cyber attacks against Georgia. *Government of the Netherlands* [online], 20 February 2020. Available from https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2020/02/20/the-netherlands-considers-russia%E2%80%99s-gru-responsible-for-cyber-attacks-against-georgia.

condemned Russia for undermining Georgia's sovereignty. Georgia,[165] along with Czechia,[166] even expressively referred to the infringement, resp. violation of sovereignty.

Additional threshold of serious adverse consequences

Another way how to determine the threshold for the due diligence obligation application is to set an additional threshold for the due diligence obligation itself. That is the way the authors of Tallinn Manual 2.0 decided to take. They used an analogy from the international environmental law holding that the due diligence obligation applies when a cyber operation (affects other States rights and furthermore) results in 'serious adverse consequences'. The Netherlands took the same position.[167] Unfortunately, the boundaries of the threshold of serious adverse consequences from the international environmental law is not transferable to the cyber context, and the experts could not further agree on the precise threshold for the identification of such consequences.[168] Nonetheless, they managed to agree that neither a presence of physical damage to objects nor injuries to individuals is required[169] and provided a series of examples that could be used for the refinement of the threshold.[170]

European countries join US, UK in condemning Russian cyber attack on Georgia. *Agenda.ge* [online], 21 February 2020. Available from https://agenda.ge/en/news/2020/540.

165 Statement of the Ministry of Foreign Affairs of Georgia. *Ministry of Foreign Affairs of Georgia* [online], 20 February 2020. Available from https://mfa.gov.ge/News/Statement-of-the-Ministry-of-Foreign-Affairs-o-(7).aspx?CatID=5.

166 See statement of Czech Ministry of Foreign Affairs on Twitter available from https://twitter.com/CzechMFA/status/1230488370528346113

167 The Netherlands: International law in cyberspace, *supra* note 108. p. 5.

168 Tallinn manual 2.0, *supra* note 1. Rule 6, para 25.

169 *Ibid.*, Rule 6, para. 28.

170 *Ibid.*, Rule 6, para. 26 – 35.

4.2 Controversial aspects of the due diligence principle in the cyber context

In this section, I analyze some controversial aspects of the due diligence principle in the cyber context. The first two subsections introduce cyber-specific aspects that are especially troublesome due to their unique nature of the cyber environment that makes them impossible to analogy to any other situation. The last subsection studies reasonableness – the fundamental aspect of the application of the due diligence principle – in the light of the specific characteristics of cyberspace and the known positions of States in this respect.

4.2.1 Transit States

The character of cyberspace enables attackers not only to use the cyber infrastructure located on the territory where they found themselves but also to use other infrastructures located all around the world remotely. The scale of such remote uses ranges from complete takeover of control over compromised devices to mere routing of data through cyber infrastructure. The mere transit of routed data represents the minimal possible use of State infrastructure and often passes through a State infrastructure without being detected by the territorial State.[171] The IGE argues that if the transit State had knowledge (actual or constructive) of the operation and could take measures to effectively terminate it, the due diligence obligation should apply and the territorial State should act accordingly.[172] The applicability of the due diligence principle to the transit States is also endorsed by Australia.[173]

171 SHACKELFORD, Scott J., RUSSELL Scott and KUEHN Andreas. Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors. In Chicago Journal of International Law, vol. 17, no. 1, 2016. p. 21.
172 Tallinn Manual 2.0, *supra* note 1. Rule 6, paras. 13–14.
173 See Chapter 3.3 of this thesis.

Shackeford, Russel and Kuehn proposed three special due diligence obligations deriving from the general due diligence principle that could be reasonably required from the transit States.[174] The first one is the monitoring of State's infrastructure and mitigating all cyber threats – a requirement the IGE categorically refuses to subsume under the general due diligence obligation in cyberspace.[175] The second one is a duty to warn the target States of operations detected in their infrastructures and the last one is a duty to cooperate with the target State to identify the source of harmful operation. Unfortunately, the duty to warn would be hindered by the fact that the transit State would not probably know which State is the target State of the operation as there might be several more transit States engaged before the malicious code reaches its target so the transit State could struggle with addressing the right State. Further, the duty to cooperate in order to identify the source of the operation would be deficient for the protection of other States' rights if it was applied alone without any other measures. And finally, monitoring of State's infrastructure is regarded as onerous and ineffective.[176]

Action ability of transit States is further complicated by the fact that most Internet traffic passes through cyber infrastructure that is owned and controlled by private Internet Service Providers. It is them who gets to the detection of malicious traffic. Effective application of the due diligence obligation requires cooperation of these private entities with States. Therefore, States should to impose obligations on the Internet Service Providers to report to them the detected malicious activity with the potential to violate other States' rights.[177] Subsequently, once a State manages to detect malicious activity routed through its infrastructure, it should act in accordance with the due diligence obligation.

174 SHACKELFORD, Scott J., RUSSELL Scott and KUEHN Andreas. Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors. In Chicago Journal of International Law, vol. 17, no. 1, 2016. p. 21.
175 Tallinn Manual 2.0, *supra* note 1. Rule 6, para. 42.
176 SCHMITT. In Defense of Due Diligence in Cyberspace, *supra* note 45. p. 80.
177 Further see also subsection 7.3.1.

4.2.2 Use of botnets

Botnet is "*a network of compromised computers, so-called 'bots', remotely controlled by an intruder, 'the botherder', used to conduct coordinated cyber operations, such as distributed denial of service operations. There is no practical limit on the number of bots that can be assimilated into a botnet*."[178] And there is also no territorial limitation of botnet. Once they are compromised, the bots controlled by the intruder cause harm unwittingly. They are often called "zombies" because they seem to function normally but, in fact, they distribute ransomware or participate in DDoS attacks. The botnet network can be composed of devices from all over the world. When a huge botnet is activated and causes violation to a State's rights, the question arises of whether individual States where bots are located shoulder the due diligence obligation in the case that the use of bots in any single State does not alone reach the threshold of seriousness triggering the due diligence obligation.[179]

Some experts of the IGE suggested that if an operation using botnet reach that threshold in total, each State where bots were located should shoulder the due diligence obligation on the basis of aggregation of operations from all the States involved in botnet. The majority of the IGE, however, concluded that aggregating operations "*would create an imbalance between the right to control territory and the duty to ensure it is not used to harm other States*"[180] and if the aggregation approach was adopted "*States could be held responsible for an internationally wrongful act based primarily upon the omissions of other States (i.e., those of the other States from which the botnet is operated).*"[181]

Indeed, States should not be expected to do more that is reasonable to expect from them taking into account particularly the exercise of sovereignty over their respective territories. Yet, the question of effectiveness of fulfilling the due diligence

178 Tallinn Manual 2.0, *supra* note 1. Glossary. p. 563.
179 *Ibid.*, Rule 6, para 29.
180 *Ibid.*, Rule 6, para. 31.
181 *Ibid.*

obligation also has its role in relation to the botnet networks. For instance, in the 2007 cyber attacks on Estonia, bots from 178 States were used. If all 178 States neutralized the zombies located on their territory, would it effectively terminate or, at least, significantly reduced harm suffered by Estonia? If so, should it be more reasonable to expect them to do so?

4.2.3 Reasonably expected State behavior in cyberspace

Due diligence is a standard of conduct. The conduct that is required under the due diligence principle is a reasonably expected conduct aimed at the protection of other States' rights. 'Reasonableness' is the cornerstone of the application of the due diligence principle. It ensures that it cannot be required from States to use measures they do not possess, and it further determines which measures are expected to be taken in particular situations and which not. The determination is based on balancing the impact of the measures on a territorial State that would take them and the gravity of the harm potentially sustained by target States. More specifically, it cannot be required from a sovereign State to take measures that would cause significant harm to itself.

In the view of the IGE, such situation could occur, for instance, if a State did not have any other measure to take than to shut down some of its essential networks in order to terminate an operation harmful to a target State. The Netherlands shared its view on the matter of reasonableness stating that "*[i]f, for example, a cyberattack is carried out against the Netherlands using servers in another country, the Netherlands may, on the basis of the due diligence principle, ask the other country to shut down the servers.*"[182] The reasonably expected diligent behavior of the territorial State notified by the Netherlands would consist of shutting down the indicated servers. At first sight, the view of the Netherlands may seem contradictory to that of the IGE. However, this conclusion would be rather hasty. While the IGE refers to "*essential*

182 The Netherlands: International law in cyberspace, *supra* note 108. p. 4.

networks", the Netherlands uses more general expression "*servers*". The difference between these two categories may be crucial. This demonstrates that the assessment of reasonableness is dependent on the detailed factual circumstances of each case.

In relation to the reasonable expectations, Australia noted that "*it may not be reasonable to expect (or even possible for) a state to prevent all malicious use of ICT infrastructure located within its territory.*" This view is generally accepted. If it were not, the due diligence standard would shift from the standard of conduct to the standard of result, which would be indeed unreasonable.[183] The debate related to the reasonableness is concerning also preventive monitoring of networks composing a State's cyber infrastructure. Most scholars deem such monitoring unreasonable to expect.

Whether the application of the due diligence principle will gain momentum in international cyber law largely depends on the adequacy of the refinement of what is reasonable to expect from States and what is not. If States were required to take unreasonably burdensome measures, they would constantly breach their due diligence obligations which could lead to an excessive use of countermeasures in response, loss of mutual confidence between States in dealing with the cyber issues and thus undermine international stability.[184] Therefore, it is of crucial importance to refine the due diligence principle in a thorough manner adequately reflecting reasonable expectations.

4.3 The content and the breach of the due diligence obligation

When the due diligence obligation is triggered, the territorial State must take all feasible measures to put an end to the operation in concern. If it failed to do so, the breach of the due diligence obligation would be constituted. It is thus of crucial

183 See Chapter 1.1 of the present thesis.
184 JENSEN, Eric T., WATTS Sean. A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?. *Texas Law Review*, vol. 95, 2017. p. 1574.

importance to bear in mind that after the activation of the due diligence obligation by the triggering elements, the obligation might be violated only by the subsequent omission of taking required measures by the territorial State. Accordingly, the omission of taking measures would not arise if there were not any available measures for the territorial State to put an end to the operation. Therefore, the feasibility of measures is a crucial aspect for the determination of the breach.

As already noted, due diligence is a flexible standard based on reasonable expectations States should meet. The behavior required under the due diligence principle differs according to the given circumstances. The factor that varies the level of required care to a great extent is the feasibility of measures a State can take. 'Feasibility' indicates the availability of reasonably expectable measures to a State in a particular situation. The due diligence principle cannot oblige States to take measures they are simply not able to take. Neither can it require taking measures that are not reasonably expectable from them. This aspect of the due diligence principle is particularly influential in cyberspace because of significant differences in the technological development of States.

The more technologically developed a State is, the more probably it will be able to take appropriate due diligence measures.[185] Accordingly, reasonable expectations, as well as due diligence standard required from the technologically advanced States, will rise. Besides, cyber infrastructure of such States is an enticing medium for conducting operations of malicious non-state actors, especially through botnets.[186] Therefore, technologically advanced States will be those who bear the heaviest burden of the due diligence obligation.

The feasibility of measures largely depends on States' cyber capabilities. When a State has more measures available to it that would satisfy the due diligence obligation, it can employ any measures it deems appropriate as long as it complies

185 Tallinn Manual 2.0, *supra* note 1. Rule 7, para 16.
186 SCHMITT. In Defense of Due Diligence in Cyberspace, *supra* note 45. p. 74.

with the due diligence obligation. Possession of some capabilities, such as blocking IP addresses located in the State territory, is widespread among States and it can be presumed that most of States are capable of taking measures like blocking certain IP addresses engaged in a malicious operation.[187] On the other hand, States may possess some particular cyber capabilities they do not want to disclose. Undoubtedly, due to the legitimate security interests, it cannot be required from States to expose all their cyber capabilities. Therefore, in some situations, States can declare themselves incapable of taking appropriate measures even though they have specific capabilities that enable them to put an end to malicious operations. Correspondingly, the protection of legitimate security interests precluding the use of secrete cyber capabilities in order to comply with the due diligence obligation is an inherent limitation of the application of the due diligence.

There might be situations when the territorial State lacks measures to put an end to the operation and other State or a group of States do have adequate capabilities to terminate the operation and are willing to assist the territorial State. This situation raises the question of whether the territorial State is obliged to request assistance from the States possessing adequate capabilities. The IGE rejected that the territorial States should bear additional obligation to request external assistance building upon the limitation of the due diligence obligation by the capacities of the sovereignty of the territorial State.

Interestingly, the IGE suggests that if a State lacked adequate capability itself, hiring an external private company having the adequate capabilities to perform the task under the territorial State's control could be an appropriate step to comply with the requirement of exhausting all feasible measures.[188] However, the use of this method would have to be reasonably justified by the elevated harm of the target State. Additionally, there are private companies that own, operate and control large parts

187 Tallinn Manual 2.0, *supra* note 1. Rule 7, para 16.
188 Tallinn Manual 2.0, *supra* note 1. Rule 7, para 17.

of States' cyber infrastructure, such as Internet Service Providers or Mobile Operators, whose abilities in relation to the confrontation of malicious uses of such parts of infrastructure are fundamental for compliance with the due diligence obligation. In the view of the IGE, States must "*exhaust all feasible means to secure the cooperation*" with these companies to comply with the due diligence obligation.[189]

189 Tallinn Manual 2.0, *supra* note 1. Rule 7, paras. 19–20.

5 Responses to the breach of the due diligence obligation

The violation of the due diligence obligation gives rise to the constitution of an internationally wrongful act under the law of State responsibility. As a consequence, the injured States are entitled to resort to lawful responses under international law against the State that breached its due diligence obligation. These self-help responses include acts of retorsion and countermeasures. It is noteworthy that France probably misread[190] Tallinn Manual 2.0 and thinking that the Manual advocated use of self-defense as a lawful response to the breach of the due diligence obligation, it expressively opposed such possibility. I comment on the background of this misunderstanding in the last section of this chapter.

5.1 Retorsion

Whereas countermeasures are measures that would be otherwise unlawful if they were not taken in response to the breach of an internationally wrongful act,[191] retorsion is conduct that is lawful but "unfriendly". Even though they are "unfriendly" in nature and may be detrimental to the interests of the States targeted by them, the acts of retorsion do not violate any international obligations.[192]

Typical measures of retorsion are limitations on diplomatic relations, such as declaring diplomats on a mission in foreign States *persona non grata* or embargos.[193] In relation to the malicious cyber activities, the United States prohibits the entry of persons involved in such activities into the United States territory.[194] With a notable

190 SCHMITT, Michael N. France's Major Statement on International Law and Cyber: An Assessment. *Just Security* [online], 16 September 2019. Available from https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/.

191 ILC Draft Articles on State Responsibility, *supra* note 36. Commentary on countermeasures, para 1.

192 *Ibid.*, Commentary on countermeasures, para 3.

193 *Ibid.*

194 Executive Order "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities". *The White House* [online]. 1 April 2015. Available from

restriction of impediments to the authorized transit to or from the United Nations headquarters,[195] there is no international law obligation granting the free entry of foreign citizens into the territory of United States. Therefore, if not used for impediments to the transit to or from the UN headquarters,[196] this measure is also an example of a measure of retorsion.[197] Additionally, retorsion could be conducted via cyber means, for instance, by blocking certain communication transmission emanating from another State.[198] The Netherlands suggest that a cyber retorsion measures could be also "*limiting or cutting off the other state's access to servers or other digital infrastructure in its territory, provided the countries in question have not concluded a treaty on mutual access to digital infrastructure in each other's territory*."[199]

Acts of retorsion are not subject to any procedural requirements under international law.[200] They are within the full discretion of States that undertake them as long as they are limited to acts that do not violate international obligations. That means that, *inter alia*, that there is no requirement of previous notification of measures of retorsion, nor limitation of duration of the measures. Moreover, the lack of procedural pre-conditions enables States to undertake retorsion "*regardless of*

---

https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

195 Agreement between the United Nations and the United States of America regarding the Headquarters of the United Nations. United Nations – Treaty Series no. 147. 26 June 1947.

196 See a recent example of such prohibited restriction here: LYNCH, Colum, GRAMER, Robbie. Trump Administration Blocks Iran's Top Diplomat From Addressing the U.N. Security Council. *Foreign Policy* [online]. 6 January 6 2020. Available from https://foreignpolicy.com/2020/01/06/trump-administration-blocks-iran-foreign-minister-zarif-addressing-un-security-council/.

197 TZANAKOPOULOS, Antonios. State Responsibility for Targeted Sanctions. *AJIL Unbound*, 113, 2019, p. 136.

Recently, the Council of the European Union adopted legislation that enables it to take measures to respond to cyber attacks, including attempted cyber attacks, on the Member States and the EU institutions. The legislation includes a measure of prevention of the entry of the sanctioned individuals into, or transit through, territories of the EU Member States.

198 SCHMITT, Michael N. Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, 2014, vol. 54, no. 3. p. 701.

199 The Netherlands: International law in cyberspace, *supra* note 108. p. 7.

200 DUPONT, Pierre-Emmanuel. Countermeasures and Collective Security: The Case of the EU Sanctions Against Iran. *Journal of Conflict & Security Law*, 2012, vol. 17. no. 3, pp. 301–336.

whether the targeted state's unwanted behavior violated international law or not."[201] In other words, "*anybody is allowed to be unfriendly as long as they do not violate the law*."[202]

5.2 Countermeasures

By contrast, there are many conditions to the lawful use of countermeasures. This is so particularly because, as noted by the ILC, "[*l*]*ike other forms of self-help, countermeasures are liable to abuse and this potential is exacerbated by the factual inequalities between States.*"[203] Some scholars see the restrictions in application of countermeasures so limiting in the cyber context that they allege that the restrictions could, in fact, encourage, States to interpret the hostile cyber operations as uses of force or armed attacks in order to broader their options of self-help remedies with a view to possibly resort to self-defense which would is difficult to employ than countermeasures.[204] Because of these restrictions that render the resort to countermeasures in the cyber realm ineffective, scholars, as well as States, proposed some modifications of the application of countermeasures, which would make them more available and more effective.

5.2.1 Purpose and character of countermeasures

Countermeasures may be employed in order to induce a State which is responsible for an internationally wrongful act to comply with its international obligations,[205] for instance, the due diligence obligation. Therefore, the purpose of countermeasures

201 TIKK, Eneken. Will Cyber Consequences Deepen Disagreement on International Law. *Temple International & Comparative Law Journal*, 2018, vol. 32, no. 2. p. 193.
202 TZANAKOPOULOS, Antonios. State Responsibility for Targeted Sanctions. *AJIL Unbound*, 113, 2019, p. 136.
203 ILC Draft Articles on State Responsibility, *supra* note 36. Commentary on countermeasures, para 2.
204 CORN, Gary, JENSEN, Eric. The use of force and cyber countermeasures. *Temple International & Comparative Law Journal*, 2018, vol. 32, no. 2. p. 129.
However, self-defense is not an instrument State might use in response to a breach of the due diligence obligation.
205 ILC Draft Articles on State Responsibility, *supra* note 36. Article 49, para. 1.

must not be the punishment of the State that breached the due diligence obligation. In addition, anticipatory countermeasures are not permitted,[206] nor countermeasures that aim to deter.[207] Further, the countermeasures are of a temporary character.[208] They must be terminated as soon as the legality of the relation between the concerned States is restored.[209] In this regard, it is important to note that if the responsible State is obligated to provide reparations to the injured State, the countermeasures may continue even though the malicious operation giving rise to the breach of the due diligence has ended.[210] In fact, countermeasures may also be employed after the termination of the operation to ensure reparation only,[211] but once the dispute in concern gets before a judicial organ, the countermeasures must be suspended without due delay.[212] The character of temporality implies that the countermeasures should be reversible.[213] However, Schmitt notes that the requirement of reversibility is not absolute, demonstrating it with an example of a DoS[214] countermeasure which "*can be terminated and service restored, but the activities that were blocked may not be able to be performed later*."[215]

5.2.2 Limitation of countermeasures

An essential limitation of countermeasures is that they shall not amount to the level of use of force, nor affect other fundamental obligations of international law.[216]

206 Although some scholars oppose this view. *Cf*. CORN, Gary, JENSEN, Eric. The use of force and cyber countermeasures. *Temple International & Comparative Law Journal,* 2018, vol. 32, no. 2. p. 131.
207 SCHMITT. Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law, *supra* note 198. p. 715.
208 ILC Draft Articles on State Responsibility, *supra* note 36. Commentary to the Article 49, para. 7.
209 *Ibid.*
210 SCHMITT. Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law, *supra* note 198. p. 715.
211 ILC Draft Articles on State Responsibility, *supra* note 36. Commentary to the Article 49, para. 8.
212 *Ibid.*, Article 52, para. 3.
213 *Ibid.*, Commentary to the Article 49, para. 9.
214 "*Denial of Service (DoS): The non-availability of computer system resources to their users. A denial of service can result from a cyber operation*." in Tallinn Manual 2.0, *supra* note 1. Glossary. p. 564.
215 SCHMITT. Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law, *supra* note 198. p. 714.
216 ILC Draft Articles on State Responsibility, *supra* note 36. Article 50.

Besides, the countermeasures must be proportional.[217] The requirement of proportionality does not reflect only the seriousness of injury suffered, but also the rights of the injured State that were violated and the gravity of the breach of the international obligation.[218] Therefore, when an injured State undertakes countermeasures on the basis of the breach of the due diligence obligation, it must take into consideration that the responsible State did not violate the injured State's sovereignty, nor breached the prohibition of intervention or prohibition of use of force,[219] even though the severity of the operation corresponded to a violation of such rights. Breaching its due diligence obligation, the responsible State failed to take measures to protect such rights, it did not violate them. This factor must be taken into account by the injured State. The ILC notes that "*the position of other States which may be affected may also be taken into consideration*."[220] This might be an interesting implication for the application of countermeasures in the cyber context overall, because cyber operations, particularly those using botnets, may target a practically unlimited number of States.[221]

5.2.3 Procedural pre-conditions to the use of countermeasures

As concerns procedural pre-conditions to the lawful use of countermeasures, Article 52 paragraph 1 of the ILC Draft Articles on State Responsibility sets two requirements of prior notifications. First, the injured State must call on the responsible State to comply with its obligations (Article 52 paragraph 1 letter a) and second, the injured State must notify the responsible State of any decision to take

217 *Ibid.*, Article 51.
218 *Ibid.*
219 SCHMITT. Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law, *supra* note 198. p. 709.
220 ILC Draft Articles on State Responsibility, *supra* note 36. Commentary to the Article 51, para. 6.
221 An example of such operation is notoriously known WannaCry ransomware campaign that affected around 150 States worldwide (see COOPER, Charles. WannaCry: Lessons Learned 1 Year Later. *Symantec* [online], 16 May 2018. Available from https://symantec-blogs.broadcom.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later?es_p=6911388).

countermeasures and offer negotiations on the issue (Article 52 paragraph 1 letter b).[222] The ILC notes that the two notifications can be made simultaneously.[223] As a practical matter of the application of the due diligence principle, these two notifications could be combined with the notification of the State targeted by malicious operation to the territorial State. Accordingly, the notification procedure would look as follows: the target State notifies the territorial State that there is an on-going cyber operation targeting the target State that emanates from the territory of the territorial State.[224] At the same time, the target State would call upon the territorial State to fulfill its due diligence obligation and notify it that if it failed to do so, it might undertake countermeasures against the territorial State.

Nevertheless, sometimes the notification of the intention to take countermeasures may render the effectiveness of countermeasures thwarted.[225] This may occur, for instance, with asset freezing. After the notification of intention to freeze assets by the injured State, the responsible State might withdraw assets from banks in the injured State, which would make the asset freezing infeasible.[226] Therefore, Article 52 paragraph 2 of the ILC Draft Articles on State Responsibility introduces an exception to the requirement of the notification of intention to take countermeasures and offering of negotiations represented by "urgent countermeasures". This exception, however, does not relate to the requirement of call upon the responsible State to comply with its obligations under Article 52 paragraph 1 letter a.

An evolving opinio iuris of States concerning the use of countermeasures as a response to hostile cyber operation moves towards the view that urgent countermeasures may be especially important because the notification pre-

222 ILC Draft Articles on State Responsibility, *supra* note 36. Article 52, para. 1.
223 *Ibid.*, Commentary to the Article 52, para. 5.
224 After such notification, the territorial State would gain knowledge of the operation in concern which is one the elements triggering the due diligence obligation.
225 ILC Draft Articles on State Responsibility, *supra* note 36. Commentary to the Article 52, para. 6.
226 *Ibid.*, Commentary to the Article 52, para. 6.

conditions are not well adaptable to the cyber context. France emphasized that "*[t]he possibility of taking urgent counter-measures is particularly relevant in cyberspace, given the widespread use of concealment procedures and the difficulties of traceability.*" The United Kingdom noted that "*where the UK is responding to covert cyber intrusion with countermeasures,*" it is not always obliged to give the prior notification because "*it could not be right for international law to require a countermeasure to expose highly sensitive capabilities in defending the country*." The UK's view is not entirely clear in what notifications the UK reserves to omit, but it seems that the UK goes beyond the concept of urgent countermeasures and suggests the possibility to derogate also the call upon the responsible State to fulfill its international obligations.

5.2.4 Collective countermeasures

Generally, an entity that may resort to countermeasures is the injured State.[227] It also seems to be clear that where is a plurality of injured States, they are entitled each individually, but may take collaborative countermeasures by a joint effort.[228] Apart from this, there is a controversy on whether non-injured States may undertake countermeasures in the general or collective interest acting at the request and on behalf of the injured States. In 2001, the ILC acknowledged that there is State practice substantiating the use of such measures, but it considered it embryonic and insufficient for the determination of a rule regulating collective countermeasures.[229] Consequently, the ILC Draft Articles remain unclear on the issue leaving it for the further development of international law.[230]

In 2019, Estonia became the first State who expressed its view on the collective countermeasures in cyberspace. Bearing in mind massive cyber attacks targeting

227 Non-state actors cannot resort to countermeasures. Potential defensive action of a non-state actor could give rise to the due diligence of a State where the non-state actor is based. See Tallinn Manual 2.0, *supra* note 1. Rule 24, para. 2.
228 Tallinn Manual 2.0, *supra* note 1. Rule 24, para 10.
229 ILC Draft Articles on State Responsibility, *supra* note 36. Commentary to Article 54, para. 6.
230 *Ibid.*

the whole country for several weeks in 2007,[231] Estonia, unsurprisingly, took an affirmative position to the use of collective countermeasures advocating that "*states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation*,"[232] noting that "*allies matter also in cyberspace.*"[233] Estonia, thus, put the "collective interest" into the spotlight, rather than "general interests". More surprisingly, France, an ally of Estonia in NATO and the EU, opposed the Estonian position noting that collective countermeasures are not permissible, which "*rules out the possibility of France taking such measures in response to an infringement of another State's rights*."[234] It is likewise noteworthy that the issue of collective countermeasures resulted too controversial to reach consensus of the IGE on the issue of their lawfulness.[235] At last, the majority argued that taking countermeasures on behalf of another State should not be lawful.[236] Additionally, the IGE examined the question of whether States may provide assistance to the injured State in conducting its countermeasures. This matter, however, was left unresolved with three different views among the Experts.[237]

5.2.5 Non-state actors targeted by countermeasures

Regardless of the lawfulness of collective countermeasures, it should remain clear that subjects entitled to resort to countermeasures are only States. Therefore, non-state actors may not undertake countermeasures.[238] That being indisputable, the

231 Estonia hit by 'Moscow cyber war'. *BBC* [online]. 17 May 2007. Available from http://news.bbc.co.uk/2/hi/europe/6665145.stm.

232 President of the Republic at the opening of CyCon 2019. *President of Estonia* [online], 29 May 2019. Available from https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html.

233 *Ibid.*

234 France: International law applied to operations in cyberspace, *supra* note 106. p. 7.

235 Tallinn Manual 2.0, *supra* note 1. Rule 24, paras. 4–9.

236 *Ibid.,* Rule 24, para. 7.

237 *Ibid.,* Rule 24, para. 9.

238 Nevertheless, it may happen that a non-state actor targeted by a cyber attack urges the State A where it is based to undertake countermeasures but the State A decides not to undertake them. Consequently, the non-state actor decides to act on its own and hack-back its attacker without consent of the State A where it is based. Such an action could violate sovereignty or other rights of the State B where the attacker is based. Being unlawfully targeted by the non-state actor, the State B

question is whether non-state actors could be targeted by countermeasures. Interestingly, Schmitt suggests that they could be.[239] He argues that "*even though international law does not permit countermeasures against non-State actors on the basis of their own actions, operations against the non-State groups or individuals may be appropriate if styled as countermeasures against the States from which they act*."[240] In other words, the real targeted subject of the defensive operation would be a non-state actor, but for the violation of the sovereignty of the State's where the non-state actor was based, the operation would qualify as countermeasures and thus would be permissible. This peculiar use of countermeasures, would, however, have to be consistent with other requirements necessary for lawful resort to countermeasures. Particularly, fulfilling the purpose of countermeasures – to induce the State responsible for the breach of its due diligence – might be questionable in these cases.

5.3 Self-defense

Resorts to self-defense were traditionally related to reactions to the armed attacks conducted by States. Nevertheless, there is an extensive practice of use of force against non-state actors.[241] Some of these actions were conducted with the consent of the States where the non-state actors were located or with the authorization of the United Nations Security Council. Such actions seem justified enough. Nevertheless, similar actions were also conducted without the consent of the territorial State.

---

could undertake countermeasures against State A if it failed to exercise its due diligence obligation in relation to the hack-back of the non-state actor. But if the State A did not fail its due diligence obligation, State B could not lawfully resort to countermeasures against State A. Nevertheless, it could resort to acts of retorsion, or act in necessity. See Tallinn Manual 2.0 , *supra* note 1. Rule 6, para. 34.

239 SCHMITT. In Defense of Due Diligence in Cyberspace, *supra* note 45. p. 79.

240 SCHMITT, Michael N. International Law and Cyber Attacks: Sony v. North Korea. *Just Security* [online], 17 December 2014. Available from https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/.

241 CHACHKO, Elena, DEEKS, Ashley. Which States Support the 'Unwilling and Unable' Test?. *Lawfare* [online], 10 October 2016. Available from https://www.lawfareblog.com/which-states-support-unwilling-and-unable-test.

Recently, such actions were conducted on the basis of the "unable or unwilling test".[242] Rather than generally accepted justification for uses of force against non-state actors, this test represents still a controversial justification for actions on the territories of sovereign States that do not agree with such uses of force on their territories. However, a growing number of States support the "unable or unwilling" doctrine,[243] and so does the majority of the IGE in relation to the most severe cyber operations.

The majority of the IGE concluded that there are situations when States may resort to self-defense even if the operation amounting to the level of armed attack cannot be attributed to a territorial State and the territorial State did not give its consent to the defensive action.[244] In the view of these Experts, the circumstances justifying the non-consensual resort to self-defense are such that the action in self-defense "*complies with the principle of necessity, is the only effective means of defence against the armed attack, and the territorial State is unable (e.g., because it lacks the expertise or technology) or unwilling to take effective actions to repress the relevant elements of the cyber armed attack. In particular, these Experts emphasized that States have a duty to ensure their territory is not used for acts contrary to international law.*"[245] The reference to the due diligence principle is somewhat confusing because the use of force under the "unable or unwilling doctrine" could be permissible not only on the territory of unwilling States (i.e. State in breach of the due diligence obligation) but also on the territory of unable States who actually comply with the due diligence obligation. The breach of the due diligence is therefore not a decisive element in the assessment of the unable or unwilling test. More importantly, the unable or unwilling doctrine

242 OHLIN, Jens D. The Unwilling or Unable Doctrine Comes to Life. *Opinio Juris* [online], 23 September 2014. Available from https://opiniojuris.org/2014/09/23/unwilling-unable-doctrine-comes-life/.
243 CHACHKO, Elena, DEEKS, Ashley. Which States Support the 'Unwilling and Unable' Test?. *Lawfare* [online], 10 October 2016. Available from https://www.lawfareblog.com/which-states-support-unwilling-and-unable-test.
244 Tallinn Manual 2.0, *supra* note 1. Rule 71, para. 25.
245 *Ibid.*

does not permit the use of force against the territorial State, but only against the non-state actor *located on the territory* of the territorial State.

It is noteworthy that France probably misread[246] Tallinn Manual 2.0 and got confused by the reference to the due diligence principle. Thinking that the Manual permits use of force against unable or unwilling States, it held that

> [t]he fact that a State does not take all reasonable measures to stop wrongful acts against other States perpetrated from its territory by non-state actors, or is incapable of preventing them, cannot constitute an exception to the prohibition of the use of force. Under these conditions, France does not recognise the extensive approach to self-defence expressed by a majority of the Tallinn Manual Group of Experts which allows a State that is victim of a large-scale cyberattack perpetrated by non-state actors from the territory of another State to use self-defence against that State... A State's failure to comply with this [due diligence] obligation is not a ground for an exception to the prohibition of the use of force.[247]

Nevertheless, the IGE did not advocate that the breach of the due diligence could justify the resort to self-defense against the territorial State.[248] The target of the self-defensive action would be a non-state actor, not the State on whose territory the actor was based. French interpretation of the Tallinn Manual 2.0 would mean that States could overcome the attribution problem solely by applying the unable or unwilling test. That would have a heavily destabilizing effect. As the Netherlands suggested, an action of self-defense could not be conducted without "*adequate proof of the origin or source of the attack and without convincing proof that a particular state or states or organised group is responsible for conducting or controlling the attack. States may*

246 SCHMITT, Michael N. France's Major Statement on International Law and Cyber: An Assessment. *Just Security* [online], 16 September 2019. Available from https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/.
247 France: International law applied to operations in cyberspace, *supra* note 106. p. 10.
248 SCHMITT, Michael N. France's Major Statement on International Law and Cyber: An Assessment. *Just Security* [online], 16 September 2019. Available from https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/.

therefore use force in self-defence only if the origin of the attack and the identity of those responsible are sufficiently certain. This applies to both state and non-state actors."[249]

To conclude, in the view of the majority of the IGE, the lack of diligence of the territorial State, i.e. its unwillingness to put an end to an operation of a non-state actor based on its territory amounting the level of the armed attack, could justify the use of force against non-state actor. Nevertheless, such lack of diligence should not justify the use of force against the unwilling territorial State. Therefore, self-defense is not a lawful response to the breach of the due diligence obligation. The only permissible reactions to the breach are acts in retorsion and countermeasures taken in compliance with the requirements of the law of State responsibility.

249 The Netherlands: International law in cyberspace, *supra* note 108. p. 9.

6 Preventive feature of due diligence

In the context of the due diligence principle, it is often discussed whether or not the principle should encompass any preventive obligations. This is so particularly because, in international environmental law, the due diligence principle has a relevant preventive feature lying in the principle of prevention. The IGE, like most of the other scholars, firmly rejects the opinion that preventive due diligence obligations should exist in cyberspace.[250] Its rejective opinion is build upon two arguments. First, the requirement to prevent all possible cyber threats would put an onerous burden on States,[251] and second, the requirement to prevent future operations would contradict the knowledge requirement.[252] These are, for sure, sound arguments. Nevertheless, they do not reflect the relevancy of the due diligence principle known from international environmental law. Therefore, in the first section of this chapter, I analyze the potential transferability of the obligation of prevention to the cyber context.

In the second section, I emphasize the role of some private entities for the adequate functioning of the due diligence principle. Because those obligated by the principle of due diligence are States, I comment on how States should treat the mentioned entities so that they adequately comply with their due diligence obligations. In addition, I assess whether the private entities should bear any portion of responsibility related to due diligence or not.

250 For an opposing opinion see e.g. STOCKBURGER, Peter Z. *From Grey Zone to Customary International Law: How Adopting the Precautionary Principle May Help Crystallize the Due Diligence Principle in Cyberspace.* 10th International Conference on Cyber Conflict CyCon X: Maximising Effects. NATO CCD COE Publications, 2018. ISBN 978-9949-9904-3-6.
251 Tallinn Manual 2.0, *supra* note 1. Rule 7, para 8.
252 Tallinn Manual 2.0, *supra* note 1. Rule 7, para 9.

6.1 Analogy of environmental principle of prevention

The use of preventive due diligence measures proved particularly convenient in international environmental law. Like malicious cyber operations, industrial and similar activities may have a negative transboundary impact. The risks of harm caused by such activities to neighboring States can be significant, and so can be the harm sustained. Because of the severity of potential harm to the environment of neighboring States and the abilities of States to control the hazardous activities, the due diligence principle is widely applied in the preventive context in the international environmental law. But is the application experience from the international environmental law transferable to the cyber context? Would it be reasonable to expect that States apply the due diligence principle to protect other States' rights from malicious cyber activities in a similar manner as they apply it in international environmental law?

In the fundamental case of international environmental law, *Trail Smelter*,[253] a Canadian smelting company based in Trail, the Dominion of Canada, near the border with the United States, greatly increased the intensity of smelting of zinc and lead ores which resulted in significant pollution of the environment of the United States.[254] In response, the American government claimed damages against the Dominion of Canada. The Arbitral Tribunal resolving the dispute laid the foundations for the application of due diligence in international environmental law by holding that "*no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of serious consequence and the injury is established by clear and convincing evidence*."[255]

253 *Trail Smelter Arbitral Tribunal Decision (United States of America v. Canada)*. 16 April 1938 and 11 March 1941. International Arbitral Awards. Vol 3. pp. 1905 – 1982.
254 *Ibid.,* p. 1917.
255 *Ibid.*, p. 1965.

The importance of the preventive feature of due diligence was emphasized in the 2010 *Pulp Mills* judgment.[256] In this judgment, the ICJ identified the principle of prevention related to environmental due diligence as a customary rule and "*part of the corpus of international law relating to the environment*" resting on the obligation of a State "*to use all the means at its disposal in order to avoid activities which take place in its territory, or in any area under its jurisdiction, causing significant damage to the environment of another State*."[257] In this context, the Court underlined a wide acceptance among States which has gained an environmental impact assessment as a tool of preventive due diligence stating that "*it may now be considered a requirement under general international law to undertake an environmental impact assessment where there is a risk that the proposed industrial activity may have a significant adverse impact in a transboundary context, in particular, on a shared resource*."[258]

Five years later, the ICJ reaffirmed the conclusions from *Pulp Mills* in the *Costa Rica* judgment[259] and broadened the scope of the activities requiring execution of environmental impact assessment (hereinafter "EIA") from the industrial activities to any activities that may have a significant adverse transboundary impact.[260] In addition, the Court held that "*if the environmental impact assessment confirms that there is a risk of significant transboundary harm, a State planning an activity that carries such a risk is required, in order to fulfil its obligation to exercise due diligence in preventing significant transboundary harm, to notify, and consult with, the potentially affected State in good faith, where that is necessary to determine the appropriate measures to prevent or mitigate that risk.*"[261]

256 *Pulp Mills, supra* note 53. pp. 14 – 107.
257 *Ibid.*, para. 205.
258 *Ibid.*, para. 204.
259 *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, I.C.J. Reports 2015, pp. 665–742.
260 *Ibid.*, para 104.
261 *Ibid.*, para 168.

The international environmental law incites to establish two preventive due diligence obligations in cyberspace. The first one is a substantial obligation inspired by the principle of prevention[262] requiring States to use all the means at their disposal in order to avoid activities which take place in the territory, or in any area under its jurisdiction, causing significant damage to other States' rights. The second one is a procedural obligation to undertake assessments of cyber activities where there is a risk of a significant transboundary impact, and, if the risk were identified, to notify and consult with the potentially harmed State the activity. The assessments should be conducted prior to the materialization of proposed cyber activities. Consequently, if a negative transboundary impact were recognized, the State would have to notify the potentially affected States and consult with them possible measures to mitigate the risks.[263]

As concerns the substantial obligation, there are two points of view on how to look at it. The first one is operation-oriented. This is the point of view taken by the IGE. The IGE sees the substantive preventive obligation as an obligation to prevent malicious cyber operations carried out by other States or non-state actors from the territorial State's cyber infrastructure. It alleges that the substantial preventive operation-oriented obligation lacks a knowledge requirement because it relates to hypothetical future cyber operations. Under this obligation, States would have to prevent malicious operations that they have no knowledge of; neither can have. I am of the same view as the International Group of Experts in this matter. Moreover, even the employment of all possible preventive measures cannot prevent malicious use of cyber infrastructure – neither monitoring of networks, nor surveillance of hacker groups' activities. The substantial preventive operation-oriented obligation would put an onerous burden on States[264] without a guarantee of the level of the

262 *Pulp Mills, supra* note 53. para. 205.
263 *Ibid.*, para. 204.
The United Nations Conference on Environment and Development, *Rio Declaration on Enviroment and Development*. 1992. Principles 17 and 19.
264 SCHMITT. In Defense of Due Diligence in Cyberspace, *supra* note 45. p. 80.

environmental protection efficiency. Therefore, it would not be reasonable to hold States responsible for not taking material steps preventing malicious cyber operations.

The other view on the substantial preventive obligation is infrastructure-oriented. Instead of avoiding malicious cyber operations, the obligation would lie in avoiding activities subject to authorization and control of territorial State that affect the security of its cyber infrastructure, making it possibly more vulnerable to uses in the malicious cyber operations against other States. The emphasis on authorization and control of the territorial State better reflects the application practice of the international environmental law. Potentially harmful activities would be activities significantly modifying State's cyber infrastructure, making it possibly more vulnerable to uses in cyber operations against other States, such as the construction of 5G networks. It is an activity requiring State authorization, and its realization bears potential risks of misuse.[265]

Nevertheless, it is not possible to imagine that States would be obliged to "avoid" the construction of 5G networks or similar activities only because there are risks of their misuse. In the normal course of events, the operation of cyber infrastructure, unlike the operation of smelters or pulp mills, does not cause any harm per se. Therefore, it would be unreasonable to require States to avoid inherently unharmful activities under the due diligence principle. The emphasis should be rather put on the exchange of best practices and information on cybersecurity and the establishment of communication channels for addressing serious cross-border incidents.

As regards the procedural obligation, the environmental impact assessment is based on the idea of high regulatory and control capacity of States related to the protection of the environment mentioned above. The assessment is conducted before a national authority authorizes the activity in concern. In the cyber context, the

265 See the introductory part of the Chapter 5 of the present thesis.

assessed activities would be those that are subject to authorization and regulatory control of State. Subsequently, if the cyber risk assessment identified potentially significant harmful impact on other States' infrastructures, the State of origin would notify the potentially affected States of this fact. In the environmental context, States of origin use to submit to the potentially affected States the whole environmental impact assessment as well as all related technical and other relevant information on which the assessment was based.[266] The environmental impact assessment is a transparent process open for public participation.[267] In contrast, disclosing the outcome of a cyber risk assessment may endanger the assessed activity. Information sharing is much more sensitive than it is in the case of EIA because it reveals vulnerabilities of essential systems and networks and it needs to be built on strong mutual trust.[268] The format of the notification and consultation process could be similar to the cross-border dependencies[269] consultation format established within the European Union.

The consultations and information exchange on cross-border dependencies and risks related to them is incorporated in Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (hereinafter NIS Directive) which sets forth that "*where an entity provides an essential service in two or more Member States, those Member States should engage in bilateral or multilateral discussions with each other. This consultation process is intended to help them*

266 *Pulp Mills, supra* note 53. para. 33.
International Law Commission, *Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries*, Yearbook of the International Law Commission, 2001, vol. II, Part 2, New York and Geneva, 2001. Article 8.
267 Article 2 of the Convention on Environmental Impact Assessment in a Transboundary Context.
268 The hesitant approach on information sharing revealed in the Guidelines for the EU Member States on information exchange on cross-border dependencies among the EU Members demonstrates how sensitive the information exchange may be even for close partners like the EU Member States.
269 In *NIS Cooperation Group Guidelines for the Member States on voluntary information exchange on cross-border dependencies*, a cross-border dependency is defined as "*a critical reliance of an essential service of an EU Member State on a network or information system that is located in another Member State, without which the given essential service is unable to function*."

assess the critical nature of the operator in terms of cross-border impact, thereby allowing each Member State involved to present its views regarding the risks associated with the services provided."[270] As a result of the consultation process, Member States gain information on their dependencies and may apply adequate measures mitigating risks related to the dependencies accordingly, *inter alia*, update their list of operators of essential services.

Although both the State potentially affected by the risk from the dependency and the State where from where the risk emanates may initiate the consultation process, the EU voluntary guidelines related to the process presume that the Member States potentially affected are those who are likely to iniciate the process and can have no expectiations towards States from where the risks emanate.[271] Moreover, because of the sensitivity of some of the shared information, States must not share all information at their disposal. They may refuse to provide information the disclosure of which may endanger their essential interests of security, to safeguard public policy and public security, and to allow for the investigation, detection, and prosecution of criminal offenses.[272] Under all circumstances, States should respect the need-to-know principle in order to avoid unnecessary information sharing amongst those who are not engaged in the consultation process.[273] The consultation should be conducted by the Member States' Single Points of Contact, bodies that shall exercise a liaison function for the purposes of cooperation under the NIS Directive.[274]

Accordingly, the subject-matter of the international procedural preventive obligation inspired by the EU consultation process would be limited to significant

270 Recital 24 of the NIS Directive.
271 EU Guidelines on voluntary information exchange on cross-border dependencies, *supra* note 269. p. 5.
272 Recital 8 of the NIS Directive.
273 EU Guidelines on voluntary information exchange on cross-border dependencies, *supra* note 269. p. 6.
274 *Ibid.*, p. 4.

cross-border dependencies. Beyond the scope of this process, the notifying State would not be obliged to take any further steps to ensure the prevention of harm to the potentially affected State. On the basis of the provided information, the potentially affected State could apply appropriate risk mitigation measures, enhance the protection of its population against the disruptions of essential services[275] and prepare itself for future incidents. The utility of such notification and consultation process is endorsed in the 2015 UN GGE report, which states that "*States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders.*"[276]

Nevertheless, as noted in the NIS Directive, information sharing on cross-border dependencies is particularly sensitive and even within the EU, where the trust between Member States is notable, the consultation process is rather descreet. Imposing an obligation to share information on vulnerabilities on States like Estonia, Ukraine or Georgia that were all recently targeted by large-scale cyber operations by their common neighbor, the Russian Federation, would be unreasonable and, in fact, unfair. Similarly, Israel, surrounded by Arabic States, has a history of mutual cyber attacks with its neighbors. Because of the high sensibility of information engaged in cyber risk assessment and unfortunate but understandable lack of trust between States in these conditions, a procedural preventive obligation inspired by the international environmental law is not adaptable to the cyber context, and it is not likely to be established soon. Therefore, notification and consultation of vulnerabilities with potential cross-border impact is likely to remain on the bilateral or regional level.

275 *Ibid.*
276 UN GGE 2015 Report, *supra* note 46. p. 9.

6.2 Role of private entities related to the preventive feature of due diligence

The prevention of malicious cyber operations occurring within certain cyber infrastructure largely depends on those who operate it as well as on the quality and security of the ICT components that are used in the infrastructure. Both operators of cyber infrastructure and producers of ICT components are private entities. Their role in the prevention of malicious cyber operations is, therefore, significant. Liu argues that they should consequently share of responsibility with States owed to the target States. This view is, however, exceptional. Nevertheless, the influential role of private entities must be reflected in relation to the due diligence principle.

Therefore, this section addresses the relations between States and private entities in relation to the compliance due diligence principle. I advocate that for guaranteeing high security of their infrastructure, States must, in particular, prudently consider which private entities they contract for building and operation of their essential infrastructure basing their preferences on security needs, and, subsequently, impose security requirements on those entities and control their compliance. Negligence of States in this area may result in security risks not only for the negligent State but also for any other State. In the last subsection, I comment on political considerations in the contracting stage States face in the case of the upcoming revolution of 5G networks.

6.2.1 Duty to report cybersecurity incidents

Private entities, such as Internet Service Providers, cloud computing service providers, or mobile network operators, have an essential role in securing cyberspace. Therefore, States use to adopt national regulations imposing obligations comprising of various security requirements on these entities.[277] The most

277 Along with the national security requirements, private entities also adopt standards and security guidelines produced by international organizations composed of representatives of industry. The

fundamental duty owed by these private entities is the duty to report severe cybersecurity incidents to the national authorities so that the authorities might help resolve the incidents.[278] This is an important way how States gain an actual knowledge of malicious operations in their cyber infrastructures that may potentially target other States and trigger their due diligence obligation. Moreover, it is also an important way how to gain constructive knowledge with respect to the anticipated future operations. Despite these important implications for the effectivity of the due diligence principle, the IGE rejected that States should have any preventive obligation resting on the adoption of national legislation requiring private entities to report incidents to the national authorities[279] and maintained that States should rather ensure the cooperation with these private entities when problems actually occur.[280]

The national authorities receiving reports are usually national Computer Emergency Response Teams (CERTs)[281] comprising of ICT experts that subsequently help to resolve the reported incidents. If incidents posed a potential transboundary threat, the national CERTs should be able to communicate these threats to their respective partners abroad. This cooperation is truly essential for timely response to cyber threats that are generally very invasive and fast-spreading. Establishing CERTs and

most used cybersecurity standards for private companies on a global scale are ISO/IEC 27000-series standards elaborated by the International Organization for Standardization and the International Electrotechnical Commission. The family of ISO/IEC 27000 standards amounts to tens of standards. Most importantly, the ISO/IEC 27001 standard introduces an information security management system providing a systematic approach to managing ICT security of private companies.

278 To see an example of national legislation on the incident reporing and subsequent processes see MINÁRIK, Tomáš, rev. JANČÁRKOVÁ, Taťána. National Cyber Security Organisation: CZECHIA. *NATO Cooperative Cyber Defence Centre of Excellence*, 2019.

279 Tallinn Manual 2.0, *supra* note 1. Rule 7, para. 12.

280 Tallinn Manual 2.0, *supra* note 1. Rule 7, paras. 19–20.

281 Glossary of Tallinn Manual 2.0 defines CERT as follows: "*A team that provides initial emergency response aid and triage services to the victims or potential victims of 'cyber operations' (see below) or cyber crimes, usually in a manner that involves coordination between private sector and government entities. These teams also maintain situational awareness about malicious cyber activities and new developments in the design and use of 'malware' (see below), providing defenders of computer networks with advice on how to address security threats and vulnerabilities associated with those activities and malware*." Such teams are regularly also called CSIRTs (Computer Security Incident Response Teams) and Computer Security Incident Response Capabilities (CSIRC).

the communication channels between them is, thus, of vital importance for the prevention of transnational harm. Therefore, many international organizations recommended their member States to prioritize these tasks.[282] Moreover, as a part of capacity-building efforts, States are encouraged to help less developed States to establish their own national CERTs.[283]

In addition, some private entities even establish their own CERTs (or CSIRTs).[284] Many of them participate in international associations founded for the purpose of information exchange on vulnerabilities, incidents, technical tools and other issues that affect the operation of CERTs. Moreover, these platforms join together private CERTs and national CERTs and facilitate their cooperation. For instance, FIRST (Forum of Incident Response and Security Teams), the largest association of CERTs, currently joins over 500 response teams – both nationals and privates – from all over the world.[285]

6.2.2 "Polluter Pays" Principle

In relation to the essential role of private entities in securing cyber infrastructure, Liu suggested that the "polluter pays" principle should be applied in cyberspace.[286] Polluter pays principle is a principle of international environmental law defined in the Rio Declaration as follows: "*National authorities should endeavour to promote the*

282 Recommendations of the UN GGE 2013 Report and the UN GGE 2015 Report (both *supra* note 46) on confidence-building measures included, *inter alia*, the enhancement of information sharing between national Computer Emergency Response Teams (CERTs) and among States on ICT security incidents in order to receive, collect, analyze and share information related to ICT incidents, for timely response, recovery and mitigation actions, or avoidance of misinterpretation of cyber operations as hostile State actions. Similar recommendation issued also the Organization for Economic Co-operation and Development in its Recommendation on Digital Security of Critical Activities adopted in 2019 and the Organization for Security and Co-operation in Europe in its 2013 Decision No. 1106 on the Initial Set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies.

283 The UN GGE 2013 Report (*supra* note 46) included an recommendation of "creating and strengthening incident response capabilities, including CERTs, and strengthening CERT-to-CERT cooperation."

284 See note 268.

285 The updated list of members of FIRST available from https://www.first.org/members/teams/.

286 Liu, *supra* note 130. pp. 197, 206, 208–213.

internalization of environmental costs and the use of economic instruments, taking into account the approach that the polluter should, in principle, bear the cost of pollution, with due regard to the public interest and without distorting international trade and investment."[287] Adopting this principle in cyberspace would partially shift the burden of preventive due diligence onto private entities.

Liu advocates that under this principle, both the individuals conducting cyber operations as well as the infrastructure operators who fail to secure their infrastructure should be liable for "cyber-pollution" causing harm to a State.[288] To make this principle function, State would have to adopt national legislation criminalizing large-scale cyber operations in order to punish the individuals conducting hostile cyber operations and to make the infrastructure operators provide reparations for insufficiently securing the private infrastructure they operate.[289]

A framework for criminalization of malicious cyber activities and cooperation in investigations is introduced in the Convention on Cybercrime of the Council of Europe, known as Budapest Convention.[290] The Budapest Convention sets of a series of measures to be taken at the national level[291] in the area of substantive criminal law (criminalization of defined criminal acts)[292] as well as procedural criminal law (investigation and collection of electronic evidence).[293] The implementation of the Budapest Convention is indeed recommendable for the purpose of prevention of malicious cyber activities.[294] At the time of writing, there are 65 State Parties to the

287 The United Nations Conference on Environment and Development, *Rio Declaration on Enviroment and Development*. 1992. Principle 16.
288 Liu, *supra* note 130. p. 210.
289 *Ibid.*
290 Council of Europe, *Convention on Cybercrime*. Council of Europe Treaty Series No.185. 23. 11. 2001.
291 See Chapter Two of the Convention on Cybercrime.
292 See Chapter Two Section One of the Convention on Cybercrime.
293 See Chapter Two Section Two of the Convention on Cybercrime.
294 BENDIEK, Annegret. *Due Diligence in Cyberspace: Guidelines for International and European Cyber Policy and Cybersecurity Policy.* Stiftung Wissenschaft und Politik, 2016. ISSN 1863-1053. p. 6.

Budapest Convention, including non-members of Council of Europe.[295] The Cybercrime Convention Committee established under the Convention ensures the effective use and implementation of the Convention.

Regarding the liability of operators of cyber infrastructure, Liu suggests that if operations were liable for security of their networks, they would increase their security standards. Thus more cyber intrusions would be prevented. But as Liu acknowledges himself, "*a private liability regime could dilute State responsibility moving questions of cyber-diligence from public international law into private international law. The principle risks 'exonerating certain subjects of international law from their share of responsibility for damage' caused by cyberattacks.*" Moreover, it would not be reasonable to make the operators "pay" for each cyber operation that targets a State and violates its rights. As noted earlier, the requirement to prevent all cyber threats is deemed unreasonable.[296]

The international due diligence obligation should not be shifted onto private infrastructure operators. Instead, States should set up domestic security requirements onto the private entities under their jurisdiction and control their compliance. Moreover, where necessary, they should prudently choose with which private entities they engage in cooperation and let them build and operate their networks. This first step in securing cyber infrastructure against potential misuses is more important than it might look at first sight. The problem here is twofold. First, insufficient safety of ICT items and networks, including neglecting of their constant patching, makes them vulnerable. And second, ICT devices might contain preinstalled backdoors, which can enable their producers to spy on them or even alter their functions or shut them down.

295 Although the Budapest Convention was negotiated by a regional international organization with restricted membership, under the Article 37 paragraph 1 of the Budapest Convention the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to the Convention.
296 See subsection 5.2.1.

6.2.3 Political considerations in securing cyber infrastructures

Currently, an essential debate is taking place on a global scale on the involvement of Huawei, a Chinese corporation, in the building of 5G networks.[297] Some States, like the United States, Australia, New Zealand, or Japan, allege that Huawei poses a security threat they are not willing to undertake. They are concerned that Huawei might use its technologies for espionage and sabotage,[298] referring to China's National Intelligence Law passed in 2017 that states that "*any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law.*"[299]

Some other States declared that they would not exclude Huawei from supplying technologies to build their 5G infrastructures. However, they also do not have full trust in the Chinese corporation. The United Kingdom allowed Huawei to supply its technology, but only to a limited extent. The Chinese company should not provide any "core" technology to the United Kingdom.[300] Similarly, France stated that it would not exclude Huawei from the competition, but it remains precautious to protect its security interests.[301]

The Huawei case demonstrates that different States apply different standards and adopt different measures to mitigate cybersecurity risks. In this sense, differences of

297 KHARPAL, Arjun. Here's which leading countries have barred, and welcomed, Huawei's 5G technology. *CNBC* [online], 25 April 2019. Available from https://www.cnbc.com/2019/04/26/huawei-5g-how-countries-view-the-chinese-tech-giant.html.

298 As emphasized in the Prague Propossals adopted in May 2019 at the Prague 5G Security Conference, "*due to the wide application of 5G based networks, unauthorized access to communications systems could expose unprecedented amounts of information or even disrupt entire societal processes*." The Prague Propossals are available from https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

299 KHARPAL, Arjun. Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice. *CNBC* [online], 4 March 2019. Available from https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

300 KELION, Leo. Huawei set for limited role in UK 5G networks. *BBC* [online], 28 January 2020. Available from https://www.bbc.com/news/technology-51283059.

301 CAMBRELENG, Boris, WILLIAMS, Stuart. France won't bar but may restrict Huawei in 5G network. *Tech Xplore* [online], 13 February 2020. Available from https://techxplore.com/news/2020-02-france-wont-bar-restrict-huawei.html.

views of what is diligent and what is not may influence international relations. The United States sees Huawei as a security threat, so it urges its allies to exclude the corporation from the access to their 5G networks entirely. It warns them that taking a different approach than the United States poses may lead to the restriction of intelligence sharing because it fears that the integrity of the shared confidential materials would be endangered by the negligent selection of a contractor.[302]

Whether or not, or under which conditions to allow a specific private company to participate in the building of a cyber infrastructure, is clearly a sovereign decision of each State. However, apart from the security concerns, economic and international political considerations are heavily involved in the policymaking on Huawei potential threat as well. Not only the United States push on other States to adopt their view on Huawei. China recently warned Germany that the exclusion of Huawei from the German 5G network would not remain without consequences referring to potential consequences for robust economic co-operation of German carmakers and Chinese companies.[303]

302 Interview With Maria Bartiromo of Mornings With Maria on Fox Business Network. *U.S. Department of State* [online], 21 February 2019. Available from https://www.state.gov/interview-with-maria-bartiromo-of-mornings-with-maria-on-fox-business-network-3/.
303 CZUCZKA, Tony, ARONS, Steven. China Threatens Retaliation Should Germany Ban Huawei 5G. *Bloomberg* [online], 15 December 2019. Available from https://www.bloomberg.com/news/articles/2019-12-14/china-threatens-germany-with-retaliation-if-huawei-5g-is-banned.

Conclusion

Cyberspace is a very complex and specific environment. It influences nearly every aspect of modern society, and the society has to adapt to it accordingly. One of the challenges brought by the growing importance of information and communication technologies is how international law should be applied in cyberspace. In this context, an adequate application of the due diligence principle has the potential to adapt international law to the new phenomena of malicious cyber operations. With mitigation of the attribution problem and facilitation of denial of safe havens of non-state actors, the due diligence principle offers valuable benefits of its application. This fact is already being reflected within international fora and States' position papers on the application of international law in cyberspace. The due diligence principle is shifting to the center of attention of the relevant debates. While more and more support the application of the due diligence principle in cyberspace,[304] at the time of writing, there is no State that opposes its application.

Nevertheless, to fulfill its purpose and to prove beneficial, the due diligence principle must be applied wisely. After analyzing the current state of the refinement of the due diligence application in the cyber context, I managed to identify three elements that trigger the due diligence obligation. These three elements are (1) use of the territorial State's territory or, (2) knowledge the territorial State has of a cyber operation that is supposed to be stopped, and (3) violation of State's rights. Each of the three elements might be adjusted by a corresponding potential adjustment (extraterritoriality, the concept of constructive knowledge, and additional threshold of serious adverse consequences) that could either extend or restrict the scope of the application of the due diligence obligation. The future use of these adjustments is

304 States that expressively supported the application of the due diligence principle in cyberspace include Argentina, Australia, Brazil, Estonia, Finland, France and the Netherlands.

dependent on the further refinement of the due diligence principle and its application in State practice.

The same may be said about cyber-specific aspects, such as the use of botnet networks and obligations of transit States, that are likely to remain controversial until State practice determines how to treat them. For the future determination of the application of the due diligence principle is particularly important what should be considered as reasonably expectable from States in given circumstances. The reasonable expectations are an underlying aspect of the due diligence principle and may also differ according to the availability of measures States are capable of employing to comply with the due diligence obligation. If they fail to comply with the obligation, the injured States may resort to acts of retorsions and countermeasures.

Examining the limits of the application of the due diligence principle in the last chapter, I advocated that the principle of prevention that forms part of the due diligence principle applied in international environmental law is not transferable to the cyber context. Furthermore, I assessed the role of certain private entities, such as Internet Service Providers or Mobile Network Operators, that have a significant impact on how the rights of other States are protected. I came to the conclusion that States should prudently consider which of these private entities they contract for building and operating their cyber infrastructures. Additionally, they should impose obligations on them, in particular, the obligation to report security incidents, so that they could satisfactorily comply with the due diligence obligation.

This thesis provided a complex study of the due diligence principle and its application in cyberspace. On the one hand, my research was limited by the absence of State practice explicitly reffering to the principle of due diligence. On the other hand, it was encouraged by the increasing attention the principle of due diligence gets in the current debates on the application of international law in cyberspace.

During the research period alone, three States expressively endorsed the application of the principle of due diligence.[305] More articulations of the views on the due diligence principle are expected to come. Hopefully, soon they will be accompanied by an adequate application of the due diligence principle in practice bringing more mutual respect and stability into the international relations.

305 See section 4.2.

Bibliography

Doctrine

SCHMITT, Michael N. (ed.). Tallinn manual 2.0 on the international law applicable to cyber operations. Second edition. New York, the United States of America: *Cambridge University Press*, 2017. ISBN 978-1-316-63037-2.

LIU, Ian Y. State Responsibility and Cyberattacks: Defining Due Diligence Obligations. *The Indonesian Journal of International & Comparative Law*, 2017. ISSN 2338-7602.

JENSEN, Eric T., WATTS Sean. A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer? *Texas Law Review*, 2017, vol. 95. pp. 1555–1577.

SCHMITT, Michael N. Grey Zones in the International Law of Cyberspace. 42:2 *Yale Journal of International Law*, vol. 42, no 2. 2017.

SCHMITT, Michael N. In Defense of Due Diligence in Cyberspace. *The Yale Law Journal Forum*, 2015.

STOCKBURGER, Peter Z. From Grey Zone to Customary International Law: How Adopting the Precautionary Principle May Help Crystallize the Due Diligence Principle in Cyberspace. In 10th International Conference on Cyber Conflict CyCon X: Maximising Effects. *NATO CCD COE Publications*, 2018. ISBN 978-9949-9904-3-6.

BENDIEK, Annegret. Due Diligence in Cyberspace: Guidelines for International and European Cyber Policy and Cybersecurity Policy. *Stiftung Wissenschaft und Politik*, 2016. ISSN 1863-1053.

Committee on Oversight and Government Reform, Will. Report from the Committee on Oversight and Government Reform on the OPM Breach, 7 September 2016.

JIRÁSEK Petr, NOVÁK Luděk and POŽÁR Josef. Výkladový slovník kybernetické bezpečnosti = Cyber security glossary. Praha: *Policejní akademie ČR v Praze*, 2015.

JUTTA, Brunnée. *S*ic utere tuo ut alienum non laedas. *Max Planck Encyclopedia of Public International Law*, 2010. DOI 10.1093/law:epil/9780199231690/e1607.

HUFFMAN, James. Private property and the constitution: state powers, public rights, and economic liberties. New York: *Palgrave Macmillan*, 2013. ISBN 978-1-137-37673-2. DOI 10.1057/97811376732.

DE BRABANDERE, Eric. Host States' Due Diligence Obligations in International Investment Law. *Syracuse Journal of International Law and Commerce*, vol. 42. 2015 pp. 319–361.

TIMO, Koivurova. Due Diligence. *Max Planck Encyclopedia of Public International Law*, 2010. DOI 10.1093/law:epil/9780199231690/e1034.

KASKA, Kadri. Trends in international law for cyberspace, *NATO Cooperative Cyber Defence Centre of Excellence*, 2019.

FRENCH, Duncan (Chair) and Tim STEPHENS (Rapporteur). ILA Study Group on Due Diligence in International Law, First Report, 2014.

FRENCH, Duncan (Chair) and Tim STEPHENS (Rapporteur). ILA Study Group on Due Diligence in International Law, Second Report, 2016.

SHACKELFORD, Scott J., RUSSELL Scott and KUEHN Andreas. Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors. *Chicago Journal of International Law*, vol. 17, no. 1, 2016.

ROSCINI, Marco. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. *Texas International Law Journal*, vol. 50, no. 2-3, 2015. pp. 233-274.

KIRGIS, Frederic L. Custom on a Sliding Scale. *The American Jurnal of International Law*, vol. 81, 1987. pp. 146-151.

GROSS, Oren. Cyber responsibility to protect: Legal obligations of states directly affected by cyber-incidents. *Cornell International Law Journal*, 2015, vol. 48, pp. 481–512.

COUZIGOU, Irène. Securing cyber space: the obligation of States to prevent harmful international cyber operations, *International Review of Law, Computers & Technology*, vol. 32, no. 1, 2018. pp. 37-57, DOI: 10.1080/13600869.2018.1417763.

H.E. Judge Rosalyn Higgins, President of the International Court of Justice. Speech to the Sixth Committee of the General Assembly, 2 November 2007.

ZIOLKOWSKI, Katharina. Confidence Building Measures for Cyberspace – Legal Implications. Tallinn: *NATO Cooperative Cyber Defence Centre of Excellence*, 2013.

MAČÁK, Kubo. Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, vol. 21, no. 3, 2016. pp. 405-428.

MAURER, Tim. Proxies and Cyberspace. *Journal of Conflict and Security Law*, vol. 21, no. 3, 2016. pp. 383-404.

BYMAN, Daniel. Passive Sponsors of Terrorism. *Survival*, vol. 47 no. 4, 2005 – 2006. pp. 117–144. DOI: 10.1080/00396330500433399.

DUPONT, Pierre-Emmanuel. Countermeasures and Collective Security: The Case of the EU Sanctions Against Iran. *Journal of Conflict & Security Law,* vol. 17. no. 3, 2012. pp. 301 – 336.

TIKK, Eneken. Will Cyber Consequences Deepen Disagreement on International Law. *Temple International & Comparative Law Journal*, vol. 32, no. 2, 2018. pp. 185 – 196.

TZANAKOPOULOS, Antonios. State Responsibility for Targeted Sanctions. *AJIL Unbound* 113, 2019. pp. 135 – 139.

CORN, Gary, JENSEN, Eric. The use of force and cyber countermeasures. *Temple International & Comparative Law Journal*, vol. 32, no. 2, 2018. pp. 127 – 134.

SCHMITT, Michael N. Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, vol. 54, no. 3, 2014. pp. 697-732.

WALTON, Beatrice A. Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law. *Yale Law Journal*, vol. 126, no. 5, 2017 pp. 1460-1519.

MINÁRIK, Tomáš, rev. JANČÁRKOVÁ, Taťána. National Cyber Security Organisation: CZECHIA. *NATO Cooperative Cyber Defence Centre of Excellence*, 2019.

ŠTURMA, Pavel (ed.). Casebook: Výběr případů z mezinárodního práva veřejného. Second edition. Praha: *Scripta iuridica No. 8,Univerzita Karlova v Praze, Právnická fakulta,* 2010. ISBN: 978-80-87146-37-8.

ŠTURMA, Pavel (ed.). Nové trendy odpovědnosti a řešení sporů v mezinárodním právu (vliv nestátních aktérů): studie z mezinárodního práva. Praha: *Univerzita Karlova v Praze, Právnická fakulta*, 2012. ISBN: 978-80-87146-73-6.

Government of the Kingdom of the Netherlands, 2019, Appendix: International law in cyberspace to the letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace. 26 September 2019.

Ministère des Armées. *International law applied to operations in cyberspace*. 2019.

Australia's International Cyber Engagement Strategy. 2017. ISBN 978-1-74322-412-0.

EGAN, Brian J. *International Law and Stability in Cyberspace*. Berkeley Law, 10 November 2016.

Internet sources

GUPTA, Arvind. A Tale of two UN Resolutions on Cyber-security. *Vivekananda International Foundation* [online], 29 April 2019. Available from https://www.vifindia.org/2019/april/24/a-tale-of-two-un-resolutions-on-cyber-security.

SUKUMAR, Arun M. The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?. *The Lawfare Institute* [online], 4 July 2017. Available from https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

The Cyber Law Toolkit. *Scenario 06: Cyber countermeasures against an enabling State*. Available from https://cyberlaw.ccdcoe.org/wiki/Scenario_06:_Cyber_countermeasures_against_an_enabling_State.

First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct [online], *United Nations Meetings Coverage*. Available from https://www.un.org/press/en/2018/gadis3619.doc.htm.

Codification Division of the Office of Legal Affairs of United Nations. League of Nations Codification Conference *United Nations* [online]. Available from http://legal.un.org/ilc/league.shtml.

Informal intersessional consultative meeting of the OEWG with industry, non-governmental organizations and academia (2-4 December 2019). *United Nations Office for Disarmament Affairs* [online], Available from

https://www.un.org/disarmament/oewg-informal-multi-stakeholder-meeting-2-4-december-2019/.

DE TOMAS COLATIN, S. A surprising turn of events: UN creates two working groups on cyberspace. *NATO Cooperative Cyber Defence Centre of Excellence* [online], 11 March 2019. Available from https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/.

KHARPAL, Arjun. Here's which leading countries have barred, and welcomed, Huawei's 5G technology. *CNBC* [online], 25 April 2019. Available from https://www.cnbc.com/2019/04/26/huawei-5g-how-countries-view-the-chinese-tech-giant.html.

KHARPAL, Arjun. Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice. *CNBC* [online], 4 March 2019. Available from https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

CAMBRELENG, Boris, WILLIAMS, Stuart. France won't bar but may restrict Huawei in 5G network. *Tech Xplore* [online], 13 February 2020. Available from https://techxplore.com/news/2020-02-france-wont-bar-restrict-huawei.html.

KELION, Leo. Huawei set for limited role in UK 5G networks. *BBC* [online], 28 January 2020. Available from https://www.bbc.com/news/technology-51283059.

CZUCZKA, Tony, ARONS, Steven. China Threatens Retaliation Should Germany Ban Huawei 5G. *Bloomberg* [online], 15 Dec 2019. Available from https://www.bloomberg.com/news/articles/2019-12-14/china-threatens-germany-with-retaliation-if-huawei-5g-is-banned.

Interview With Maria Bartiromo of Mornings With Maria on Fox Business Network. *U.S. Department of State* [online], 21 February 2019. Available from

https://www.state.gov/interview-with-maria-bartiromo-of-mornings-with-maria-on-fox-business-network-3/.

SMITH, Brad. The need for a Digital Geneva Convention. *Microsoft* [online], 14 February 2017. Available from https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.00018k1n01i3tfomwyo20tis4co2l.

UK condemns Russia's GRU over Georgia cyber-attacks. *GOV.UK* [online], 20 February 2020. Available from https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks.

The United States Condemns Russian Cyber Attack Against the Country of Georgia. *U.S. Department of State* [online], 20 February 2020. Available from https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/.

"Cyber Security as a Dimension of Security Policy". Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London. *Federal Foreign Office* [online], 18 May 2015. Available from https://www.auswaertiges-amt.de/en/newsroom/news/150518-ca-b-chatham-house/271832.

ROGUSKI, Przemysław. Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace. *Just Security* [online], 6 March 2020. Available from https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/.

Georgia hit by massive cyber-attack. *BBC* [online], 28 October 2019. Available from https://www.bbc.com/news/technology-50207192.

Statement of the Ministry of Foreign Affairs of Georgia. *Ministry of Foreign Affairs of Georgia* [online], 20 February 2020. Available from

https://mfa.gov.ge/News/Statement-of-the-Ministry-of-Foreign-Affairs-o-(7).aspx?CatID=5.

Statement of the Polish MFA on cyberattacks against Georgia. *Ministry of Foreign Affairs of Republic of Poland* [online], 20 February 2020. Available from https://www.gov.pl/web/diplomacy/statement-of-the-polish-mfa-on-cyberattacks-against-georgia.

The Netherlands considers Russia's GRU responsible for cyber attacks against Georgia. *Government of the Netherlands* [online], 20 February 2020. Available from https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2020/02/20/the-netherlands-considers-russia%E2%80%99s-gru-responsible-for-cyber-attacks-against-georgia.

European countries join US, UK in condemning Russian cyber attack on Georgia. *Agenda.ge* [online], 21 February 2020. Available from https://agenda.ge/en/news/2020/540.

DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, *United States Department of Defense* [online], 2 March 2020. Available from https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

COOPER, Charles. WannaCry: Lessons Learned 1 Year Later. *Symantec* [online], 16 May 2018. Available from https://symantec-blogs.broadcom.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later?es_p=6911388.

SCHMITT, Michael N. France's Major Statement on International Law and Cyber: An Assessment. *Just Security* [online], 16 September 2019. Available from https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/.

United Nations: Recent Developments in the Field of Information and Telecommunications in the Context of International Security. *INCYDER* [online]. Available from https://ccdcoe.org/incyder-articles/united-nations-recent-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security/#footnote_3_2548.

The UN GGE on Cybersecurity: What is the UN's role? *Council on Foreign Relations* [online], 15 April 2015. Available from https://www.cfr.org/blog/un-gge-cybersecurity-what-uns-role.

Update on Sony Investigation. *FBI.gov* [online], 14 December 2014. Available from https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

North Korea: Sony hack a righteous deed but we didn't do it. *The Guardian* [online], 7 December 2014. Available from https://www.theguardian.com/world/2014/dec/07/north-korea-sony-hack-a-righteous-deed-but-we-didnt-do-it.

BOORSTIN, Julia. The Sony hack: One year later. *CNBC* [online], 24 November 2015. Available from https://www.cnbc.com/2015/11/24/the-sony-hack-one-year-later.html.

RUSHE, Dominic, LAUGHLAND, Oliver. Sony cyber attack linked to North Korean government hackers, FBI says. *The Guardian* [online], 19 December 2014. Available from https://www.theguardian.com/us-news/2014/dec/19/north-korea-responsible-sony-hack-us-official.

ZETTER, Kim. Critics Say New Evidence Linking North Korea to the Sony Hack Is Still Flimsy. *Wired* [online], 1 August 2015. Available from https://www.wired.com/2015/01/critics-say-new-north-korea-evidence-sony-still-flimsy/.

SCHMITT, Michael N. International Law and Cyber Attacks: Sony v. North Korea. *Just Security* [online], 17 December 2014. Available from https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/.

CHACHKO, Elena, DEEKS, Ashley. Which States Support the 'Unwilling and Unable' Test?. *Lawfare* [online], 10 October 2016. Available from https://www.lawfareblog.com/which-states-support-unwilling-and-unable-test.

OHLIN, Jens D. The Unwilling or Unable Doctrine Comes to Life. Opin*io Juris* [online], 23 September 2014. Available from https://opiniojuris.org/2014/09/23/unwilling-unable-doctrine-comes-life/.

Executive Order "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities". *The White House* [online]. 1 April 2015. Available from https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

LYNCH, Colum, GRAMER, Robbie. Trump Administration Blocks Iran's Top Diplomat From Addressing the U.N. Security Council. *Foreign Policy* [online]. 6 January 6 2020. Available from https://foreignpolicy.com/2020/01/06/trump-administration-blocks-iran-foreign-minister-zarif-addressing-un-security-council/.

Estonia hit by 'Moscow cyber war'. *BBC* [online]. 17 May 2007. Available from http://news.bbc.co.uk/2/hi/europe/6665145.stm.

President of the Republic at the opening of CyCon 2019. *President of Estonia* [online], 29 May 2019. Available from https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html.

United Kingdom Attorney General's Office. *Cyber and International Law in the 21st Century* [online]. 23 May 2018. Available from

https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

Ministry of Defense of the Kingdom of the Netherlands. *Keynote address by the Minister of Defence, Ms. Ank Bijleveld, marking the first anniversary of the Tallinn Manual 2.0 on the 20th of June 2018* [online]. 20 June 2018. Available from https://english.defensie.nl/downloads/speeches/2018/06/21/keynote-address-by-the-minister-of-defence-ms.-ank-bijleveld-marking-the-first-anniversary-of-the-tallinn-manual-2.0-on-the-20th-of-june-2018.

Case-law

Corfu Channel case, Judgment of 9 April 1949. I.C.J. Reports 1949.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment, I.C.J. Reports 1986.

Trail Smelter Arbitral Tribunal Decision (United States of America v. Canada). 16 April 1938 and 11 March 1941. Reports of International Arbitral Awards. Vol III. p. 1905.

United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), Judgment, I.C.J. Reports 1980, p. 3.

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 43.

Gabčíkovo-Nagymaros Project (Hungary/Slovakia), Judgment, I.C.J. Reports 1997, p. 7.

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, I.C.J. Reports 2015, pp. 665 – 742.

Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, I.C.J. Reports 2010, pp. 14 - 107.

Alabama claims of the United States of America v. Great Britain, Arbitration Award rendered on 14 September 1872 by the tribunal of arbitration established by Article I of the Treaty of Washington of 8 May 1871, Reports of International Arbitral Awars, Volume XXIX. pp.125-134.

United States Department of State, Office of the Historian, *Case presented on the part of the government of Her Britannic Majesty to the tribunal of arbitration, constituted under Article 1 of the treaty concluded at Washington on the 8th May, 1871, between Her Britannic Majesty and the United States of America,* Papers Relating to the Foreign Relations of the United States, Transmitted to Congress with the Annual Message of the President, December 2, 1872, Part II, Volume I.

Island of Palmas case (United States of America v. Netherlands), 4 April 1928, Reports of International Arbitral Awards, VOLUME II. pp. 829-871.

Sambiaggio Case, 1903, Reports of International Arbitral Awards, Volume X. pp. 499-525.

Thomas H. Youmans (U.S.A.) v. United Mexican States, 23 November 1926, Reports of International Arbitral Awards, Volume IV. pp. 110-117.

Laura M. B. Janes et al. (U.S.A.) v. United Mexican States, 16 November 1925, Reports of International Arbitral Awards, Volume IV. pp. 82-98.

H. G. Venable (U.S.A.) v. United Mexican States, 8 July 1927, Reports of International Arbitral Awards, Volume IV. pp. 219-261.

The Case of the S.S. "Lotus" (France v. Turkey), 7 September 1927, Permanent Court of International Justice, Series A. - No. 10.

Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area, 1 February 2011, Seabed Dispute Chamber of the International Tribunal of the Law of the Sea, Case No. 17.

Kenneth P. Yeager v. The Islamic Republic of Iran, 2 November 1987, Iran-US Claims Tribunal, Award No. 324-10199-1.

Other

Government of the Kingdom of the Netherlands, 2019, Appendix: International law in cyberspace to the letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace. 26 September 2019.

Ministère des Armées. *International law applied to operations in cyberspace*. 2019.

Australia's International Cyber Engagement Strategy. 2017. ISBN 978-1-74322-412-0.

EGAN, Brian J. *International Law and Stability in Cyberspace*. Berkeley Law, 10 November 2016.

Council of Europe, *Convention on Cybercrime*. Council of Europe Treaty Series No.185. 23. 11. 2001.

United Nations General Assembly, Resolution 55/63, *Combating the criminal misuse of information technologies*, A/RES/56/121. 4 December 2000.

United Nations General Assembly, Resolution 56/121, *Combating the criminal misuse of information technologies*, A/RES/56/121. 19 December 2001.

United Nations General Assembly, Resolution 53/70, *Developments in the field of information and telecommunications in the context of international security*, A/RES/53/70. 4 December 1998.

United Nations General Assembly, Resolution 58/32, *Developments in the field of information and telecommunications in the context of international security*, A/RES/58/32. 8 December 2003.

United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/65/201. 30 July 2010.

United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98. 24 June 2013.

United Nations General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174. 22 July 2015.

Agreement between the United Nations and the United States of America regarding the Headquarters of the United Nations. United Nations – Treaty Series no. 147. 26 June 1947.

Organization for Security and Co-operation in Europe Permanent Council, *Decision No. 1106 Initial Set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies,* PC.DEC/1106. 2013.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal of the European Union, L 194/1.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, Official Journal of the European Union, L 151/15.

United Nations Security Council, Resolution 1373, S/RES/1373. 28 September 2001.

International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, New York and Geneva: *Yearbook of the International Law Commission*, vol. II, part 2, 2001. also published as an annex to United Nations General Assembly Resolution 56/83 *Responsibility of States for Internationally Wrongful Acts*, A/56/10 (12 December 2001).

International Law Commission, Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, New York and Geneva*: Yearbook of the International Law Commission,* vol. II, Part 2, 2001.

International Law Commission, Draft principles on the allocation of loss in the case of transboundary harm arising out of hazardous activities, with commentaries, New York and Geneva: *Yearbook of the International Law Commission,* vol. II, Part 2, 2006.

Preparatory Committee for the Codification Conference, First Report submitted to the Council by the Preparatory Committee for the Codification Conference, *Conference for the Codification of International Law*. 1929.

International Law Commission, Report of the Commission to the General Assembly on the work of its fifty-first session, New York and Geneva: *Yearbook of the International Law Commission* 1999, Volume II, Part 2, A/CN.4/SER.A/1999/Add.l (Part 2), 2003.

The United Nations Conference on Environment and Development, *Rio Declaration on Enviroment and Development*. 1992.

United Nations Economic Commission for Europe, Convention on Environmental Impact Assessment in a Transboundary Context. 1991.

The United Nations First Committee (Disarmament and International Security) of the General Assembly, Advancing responsible State behaviour in cyberspace in the context of international security, A/C.1/73/L.37. 18 October 2018.

The United Nations First Committee (Disarmament and International Security) of the General Assembly, Developments in the field of information and telecommunications in the context of international security, A/C.1/73/L.27/Rev.1. 29 October 2018.

ISO/IEC 27001 Information security management. *International Organization for Standardization* [online]. Available from https://www.iso.org/isoiec-27001-information-security.html.

ISO/IEC 27002:2013 [ISO/IEC 27002:2013]. *International Organization for Standardization* [online]. Available from https://www.iso.org/standard/54533.html.

NIS Cooperation Group, *Guidelines for the Member States on voluntary information exchange on cross-border dependencies*, CG Publication 01/2019, 2019.

NIS Cooperation Group, *Identification of Operators of Essential Services: reference document on modalities of the consultation process in cases with cross-border impact*, CG Publication 07/2018, July 2018.

National Institute of Standards and Technology, Guide for Conducting Risk Assessments, NIST Special Publication 800-30 Revision 1, 17 September 2012.

Statementby Ambassador Janne Taalas at the second session of the open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, 10 and 11 February 2020.

The Application of the Due Diligence Principle in Cyberspace

Abstract

The due diligence principle is a well-established general principle of international law. The adequacy of its use proved in many special regimes of international law, especially in international environmental law. Cyberspace is another regime where the application of the due diligence principle is desirable. An adequate application of the due diligence principle might mitigate the problem of attribution of cyber operations and help in denying safe havens of non-state actors, who conduct malicious operations in cyberspace. The adequacy of the application of the due diligence principle in cyberspace is further indicated by the results of discussions in international fora and by the emerging trend of support of the application in official declarations of States on the application of international law in cyberspace. The thesis further suggests how the due diligence principle should be applied by introducing three elements that trigger the due diligence obligation and three possible adjustments to them. It also identifies the essence of some controversial aspects of the application of the due diligence principle and introduces cyber-specific considerations for the determination of breaches of the due diligence obligation and evaluation of lawfulness of responses to the breach, which consist of acts of retorsion and countermeasures. Lastly, it explains why the principle of prevention, which forms part of due diligence in international environmental law, is not transferable to the cyber context, and what is the role of private entities in relation to the due diligence principle.

Keywords

due diligence – cyberspace – countermeasures

Aplikace principu náležité péče v kybernetickém prostoru

Abstrakt

Princip náležité péče je ustálený obecný princip mezinárodního práva. Jeho použití se osvědčilo v mnoha zvláštních režimech mezinárodního práva, zvláště v mezinárodním právu životního prostředí. Kybernetický prostor je dalším režimem, kde se aplikace principu náležité péče zdá žádoucí. Vhodná aplikace principu náležité péče by mohla zmírnit problém přičitatelnosti kybernetických operací a také pomoci v odstraňování bezpečných přístavů nestátních aktérů provádějících škodlivé kybernetické operace. Vhodnost použití principu náležité péče je dále možno dovozovat z výsledků diskuzí na půdě mezinárodních organizací a nastupujícího trendu podpory aplikace principu v oficiálních prohlášeních států ohledně aplikace mezinárodního práva v kybernetickém prostoru. Tato diplomové práce dále navrhuje, jak by měl být princip náležité péče aplikován. Uvádí tři prvky, které dávají vzniknout povinnosti náležité péče a tři možné přizpůsobující prvky k nim. Práce také představuje podstatu některých sporných aspektů aplikace principu náležité péče a upozorňuje na okolnosti specifické pro kybernetický prostor, které je třeba brát v potaz při určování porušování povinnosti náležité péče a vyhodnocování oprávněnosti reakcí na takové porušení. Práce také vysvětluje, proč princip prevence, který je součástí náležité péče v mezinárodním právu životního prostředí, není převoditelný do kybernetického kontextu, a jakou roli při plnění povinnosti náležité péče zaujímají soukromé entity.

Klíčová slova

náležitá péče – kybernetický prostor – protiopatření