VYTAUTO DIDŽIOJO UNIVERSITETAS
MCMXXII

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

CAN THE CONCEPT OF DUE DILIGENCE CONTRIBUTE TO SOLVING THE PROBLEM OF ATTRIBUTION WITH RESPECT TO CYBER-ATTACKS CONDUCTED BY NON-STATE ACTORS WHICH ARE USED AS PROXIES BY STATES?

Aurimas Kavaliauskas[1]
DOI: https://doi.org/10.7220/2029-4239.26.1

SUMMARY

This article aims to explore whether the concept of due diligence can contribute to solving the problem of attribution with respect to cyber-attacks conducted by proxies. The relevance of this article is evident from the fact that there are recent developments in State practice concerning the drafting of international cyber law rules, including the duty of due diligence, though still many questions remain open and such developments lack clarity and comprehensiveness.

To reach the aim, this article is divided into three main sections, each of which deals with a particular issue necessary to answer for the final conclusion formulation. I section briefly explores the concept of State responsibility and attribution applicable in the cyber domain. It shows the issues and challenges, highlights the problem, and suggests that due diligence might be an answer to the old problem. II section analyzes due diligence applicability. Research of new State practice is done, scholars work, and doctrine is analyzed and applied to prove the applicability and binding nature of the concept. III section describes conditions of due diligence under general international law and then goes deeper into the essence of due diligence conditions in the cyber domain. Key points are analyzed, and issues are highlighted.

Analysis has confirmed that, firstly, the State responsibility issue exists because old attribution rules are not suitable for cyber-domain. Then the State practice research, scholars' work analysis, and doctrine interpretation have confirmed that due diligence is applicable and is binding. Finally, peculiarities of cyber due diligence were studied, and practical application possibility was discussed. The conclusion is that even though further development of the concept

[1] Author is a recent graduate of Vytautas Magnus University law faculty (master's degree studies) and a lawyer in IT company.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

domain specifics is urgently needed, the concept still may be one of the possible contributors to solve the State responsibility issue.

KEY WORDS

Cyber due diligence, state responsibility for cyber-attacks, non-state actors.

INTRODUCTION

Legal problem and relevance of the work. Today there is a consensus among States that the cyber domain is a domain of warfare. Countries are developing their capabilities in the cyber domain. More and more sophisticated cyber-attacks occur. However, to this day, no State was held *de jure* responsible, which is an issue. It is not a secret that States are using proxies for their cyber agenda to avoid responsibility.

Generally, under international law, State responsibility is established according to the attribution rules envisaged in the ARSIWA (Articles on State Responsibility for internationally wrongful acts) drafted by ILC (International Law Commission). However, it is accepted that attribution rules are very stringent, and in most cases, the threshold that needs to be reached to prove the link is even impossible to reach. This is especially evident when modern technologies are used, and it is easy to mask the conduct. New ways how to establish responsibility and thus end impunity are needed. The principle of due diligence might be one of the possible ways.

The relevance of the problem is proved by the fact that the States started to reach a consensus that an inevitable norm drafting process is needed. This is evident from the work of GGE (Group of Governmental Experts) and OEWG (Open-ended Working group). In these two groups, States agreed that the use of proxies and attribution is an issue that needs to be solved, as well States agreed that due diligence is also an important principle. The relevance of the issue is also evident as the latest reports by these groups were presented in 2021. More individual State practice is published (during GGE and OEWG reports drafting process), nevertheless, it remains ambiguous. Thus, scholars need to pay more attention to the topic and try to solve contemporary international law issues.

Hypothesis of the work. The concept of due diligence is one of the alternatives to eliminate impunity, this principle is applicable with respect to cyber operations, and its application is a more convenient way to establish State responsibility due to its more liberal application.

Purpose of the work is to examine if an alternative way of due diligence based responsibility might fit this domain and contribute to solving the issue of attribution by analysing the applicability and application of the principle.

Structure of the work. This article is constructed from three main parts. In the first part, it will be briefly looked at what the key issues with the law of State responsibility are. In the second part, the applicability of the due diligence concept will be analysed. The disagreements between State practice will be analysed, the doctrine and scholars' writings will be reviewed, and an answer will be provided if the concept is binding in the cyber domain. The third part will focus on the essence of cyber due diligence and its application. It will be looked at the main conditions

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

to establish responsibility for due diligence violation, the disagreements among the scholars, how such violation may be proved, and the main struggles in applying this principle.

INTERNATIONAL LAW OF STATE RESPONSIBILITY, ITS APPLICATION, AND PROBLEMATIC IN THE CYBER DOMAIN WITH RESPECT TO ATTACKS CONDUNTED BY PROXIES

Limited functionality of attribution rules in cyberspace

To this date[2], no State was *de jure* held responsible for a cyber-attack performed by a non-state actor on behalf of a particular State, and no legal attribution was established. Although there is a number of examples when one State (or even a group of States) accuses another for its organization of cyber-attacks, neither of them referred to hard, i. e., binding, rules of State responsibility.[3] Dennis Broeders et al. think that "the absence of references to international law in the existing accusations also diminishes the value of international law as an instrument aimed at preventing conflict in cyberspace"[4] so even when there is an official *de facto* accusation from one State to another, they are still reluctant to invoke legal arguments or mechanisms, and this diminishes the vague itself attribution concept. However, not only the lack of endorsement of international law on State responsibility but also the attribution mechanism and nature of cyber-attacks itself burdens the issue.

It should be turned to the scholars' position, why they think this attribution problem exists at all. First, it exists due to an extremely high threshold of evidence and proof.[5] Lorraine Finlay and Christian Payne note "[s]imply financing a cyberattack or providing a safe haven to nonstate perpetrators would not appear to meet the threshold for the state itself to be held responsible for a cyberattack."[6] As Michael N. Schmitt and Liis Vihul states, "neither providing malware or

[2] The article is written in winter of 2022.

[3] See: *"Declaration by the High Representative on Behalf of the European Union on Respect for the EU's Democratic Processes."* https://www.consilium.europa.eu/en/press/press-releases/2021/09/24/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-respect-for-the-eu-s-democratic-processes/ [Accessed January 17, 2022]; Dustin Volz, *"U.S. Blames North Korea for 'WannaCry' Cyber Attack."* Reuters, https://www.reuters.com/article/us-usa-cyber-northkorea-idUSKBN1ED00Q [Accessed January 17, 2022]; *"U.S. Blames Russia for 'NotPetya' Cyber-Aatack,"* https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/ [Accessed January 17, 2022]; François Delerue, *Cyber Operations and International Law*, Cambridge Studies in International and Comparative Law, Cambridge: (Cambridge University Press, 2020) p. 180. **[Delerue]**.

[4] Dennis Broeders, Els De Busser and Patryk Pawlak, "Three Tales of Attribution in Cyberspace: Criminal Law, International Law and Policy Debates" (April 1, 2020). *The Hague Program for Cyber Norms Policy Brief*, p. 8. **[Broeders et al]**.

[5] Lorraine Finlay and Christian Payne, "The Attribution Problem and Cyber Armed Attacks," *AJIL Unbound* 113 (2019): 202–6 p. 205.

[6] Ibid.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

hardware nor providing the group with financing for its cyber operations are enough."[7] Dennis Broeders et al. says, "[g]iven that malicious cyber activities are perpetrated also by non-state actors who may act as proxies for the state, there is a challenge of establishing a sufficient link between the two."[8] Nori Katagiri says: "[t]here are simply too many things that nonstate attackers can do to hinder the verification process; as such, no state has stepped forward with sufficient evidence to trigger the UN Charter Article 2(4) or pursued perpetrators to prosecute in international courts."[9,10] Hathaway says that "[a]s long as the doctrine of state responsibility for the actions of non-state actors remains unclear, states can exploit that uncertainty to make an end-run around their own legal obligations."[11] These ideas refer to the challenging concept of control tests and evidence required to establish attribution. Hence, one could say that even when there is a clear State involvement, which is substantial, it is not enough to hold that State responsible under general rules of attribution. Secondly, the problem exists due to technical difficulties of traceability of attack.[12] As Kristen E. Eichensehr points out, "[f]or example, the anonymity the Internet fosters makes attributing attacks to the real-world identity of attackers difficult (though not impossible)."[13] Delbert Tran says, "structural design of the internet and the nature of information transmission across networks complicates attribution efforts."[14] On the other hand, Delbert Tran also mentions that the technological problem is "overstated".[15] Even if, by today, it is possible to track the attack,[16] the legal aspect of attribution remains. In any case, both issues combined lead to a very complicated attribution process. Therefore, it could be said that problems with state responsibility rules exist, and it is due to the ambiguous or complicated doctrine of State responsibility, and the nature of cyber-attacks themselves which make it even harder to apply the imperfect doctrine.

Looking into the article 8 of ARSIWA we see three terms, *"instructions," "direction,"* and *"control,"* which under ILC commentary are disjunctive, and attribution could be established on any of these.[17] International courts have provided its interpretation of this article, and certain main

[7] Michael N. Schmitt and Liis Vihul, "Proxy Wars in Cyber Space: The Evolving International Law of Attribution" I(II) *Fletcher Security Review* 55-73, (May 31, 2014), p. 72.

[8] Broeders et al p. 6.

[9] Nori Katagiri, "Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks," *Journal of Cybersecurity* 7, no. 1 (2021), p. 5.

[10] Broeders et al p.14.

[11] Oona A. Hathaway, Emily Chertoff, Lara Dominguez, Zachary Manfredi, Peter Tzeng, "Ensuring Responsibility: Common Article 1 and State Responsibility for Non-State Actors," *Texas Law Review* 95, no. 3 (February 2017): 539-590 p. 542.

[12] Supra note 4 p. 203; Eric F Mejia, "Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework," *Strategic Studies Quarterly* 8, no. 1 (2014): 114–32 p. 121.

[13] Kristen E Eichensehr, "Cyberwar & International Law Step Zero" *Texas International Law Journal* 50, no. 2-3 (Spring-Summer 2015): 357-380 p. 376.

[14] Delbert Tran "The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack" 20 *YALE J. L. & TECH.* 50: 376-441 p. 387.

[15] Ibid. p. 393.

[16] "Office of the Director of National Intelligence A Guide to Cyber Attribution - Dni.gov," https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf [Accessed January 18, 2022].

[17] International Law Commission Articles on Responsibility of States for Internationally Wrongful Acts, 56th Sess., A/RES/56/83 (2002) article 8 commentary 7 {ARSIWA].

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

rules could be drawn from those decisions. ICJ practice shows that the application of article 8 is quite ambiguous. However, this article will not analyze the peculiarities and ambiguities of attribution mechanism under article 8, Kubo Mačák provides a very good overview of the issue,[18] rather, this article will limit itself by only stating that it is practically impossible or at least not feasible to establish responsibility under standard rules provided in ARSIWA. This reflects the position of quite a number of scholars who research cyber law, and the topic is already quite well covered.

Alternative route to responsibility – due diligence concept

Considering all the difficulties with the ambiguous doctrine of State responsibility and considering that it might not be possible to attribute State-sponsored attacks, international law might provide another option, a backdoor, for State responsibility. It is a due diligence concept that is well known from the Corfu Channel case.[19] This principle is also reflected in the GGE report[20] and in Tallinn Manual 2.0 rule 6. Scholars also welcome this concept in the cyber domain as a possibility to solve the responsibility problem.[21]

Due diligence implies an obligation: "States must exercise due diligence in ensuring territory and objects over which they enjoy sovereignty are not used to harm other States."[22] If a State fails to comply with such a principle, it might be held responsible.[23] This is a well-established concept under environmental law. It also finds application in international law of the sea, investment law, and other legal regimes. Also, it has a significant correlation with State sovereignty and obligations arising from it.[24] However, the application of such rule in the cyber domain is subject to some questions, for instance, if it finds application at all, how it applies and what are regime specific peculiarities. All these questions will be analysed in the following sections.

[18] See Kubo Mačák, "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* 21, no 3, Winter 2016: p.p. 405–428.

[19] Corfu Channel (United Kingdom v Albania) (Merits) [1949] ICJ Rep 4, p. 22. **[Corfu]**.

[20] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/79/174 (22 July 2015) 13(c) [GGE 2015 Report].

[21] Antonio Coco, Talita de Souza Dias, "Cyber Due Diligence: A Patchwork of Protective Obligations in International Law." *European Journal of International Law* 32, no. 3 (2021): 771–806, pp. 771-772 **[Coco and Dias]**.

[22] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: (Cambridge University Press, 2017) 6 30 [Tallinn Manual Rule].

[23] Supra note 20 p. 776.

[24] Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, (Perm. Ct. Arb. 1928) p. 839 [Island of Palmas].

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

DUE DILIGENCE CONCEPT ACCEPTANCE AND APPLICABILITY IN THE CYBER DOMAIN

Before analysing the exact application of the due diligence concept, answering questions about how it works and applies, what exact obligations territorial States have, and what could be the consequences for failure to comply with such obligations, the applicability of the concept in the cyber domain first needs to be analysed. As there is no obligatory legal document that would stipulate exact binding obligations for States in the cyber domain, one could only rely on general international law, the practice of States, case law and scholars' work to answer if the due diligence concept is applicable. If due diligence applies as a general principle of law or customary rule is also a challenging and complex question, however, this article will not go deep into this, nevertheless, unavoidably, some analysis will be done. For the avoidance of doubt, this article will refer to due diligence as a concept and obligation (irrespective of its' nature according to article 38 of ICJ Statute) for a State.

Analysis of state practice and scholars' position on the applicability of the due diligence concept

The most relevant, collective, non-binding documents agreed upon between States to date are the 2015 and 2021 GGE reports. In a 2015 report, it is stated: "[s]tates should not knowingly allow their territory to be used for internationally wrongful acts using ICTs."[25] The biggest issue with this statement is that it is envisaged in a report which stipulates "voluntary, non-binding norms."[26] Report published in 2021 failed to confirm binding nature of the obligation (although it provided more guidance of possible way how this concept applies). Thus, the situation is that there is no mutually and jointly accepted consensus stipulated in a legally binding document on concept applicability as a binding norm. However, State practice expressed while drafting certain reports might serve as a valuable source that needs to be analysed.

I. State practice in favour of concept binding nature

Group of States confirms and acknowledges the concept applicability in the cyber domain. The Netherlands position: "The Netherlands, however, does regard the principle as an obligation in its own right, the violation of which may constitute an internationally wrongful act."[27] Japan position: "States have a due diligence obligation regarding cyber operations under international

[25] GGE 2015 Report 13(c).
[26] Ibid. 13.
[27] "Letter to the Parliament on the International Legal Order in Cyberspace." Parliamentary documeny, Ministerie van Algemene Zaken, https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace appendix at 4, [Accessed February 4, 2022].

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

law."[28] Similar views are expressed by other States – France,[29] the Czech Republic,[30] Estonia,[31] Germany,[32] Norway,[33] Romania,[34] Switzerland,[35] Finland,[36] Australia.[37] Republic of Korea, for instance, states : "[t]he ROK believes that the international community should embark on discussions to review the legal status of due diligence to be elevated as a legal obligation."[38] This statement might presume that currently there is no general agreement among States on the legal status of the due diligence concept, however, one State's position cannot constitute a fact. In general, these States accept the applicability of the concept, however, some of the States also question how it should apply.

There is also a joint position on behalf of the EU.[39] This statement by High Representative Josep Borrell, although made in the context of the Covid-19 pandemic, provides valuable information. By this statement, countries were encouraged to exercise due diligence. Even though it could be questioned what legal value such a statement might give, as it was not firmly said that due diligence exists as an obligation, it still adds value to the overall discussion. Also, in 2011 Council of Europe (one of the Ministers Committee) adopted an important recommendation in which due diligence obligation was stipulated.[40] Some valuable information could be found in a report made by Duncan B. Hollis. This report analysed how State members of OAS understand the application of international law in the cyber domain. In this report it was constituted: "Chile, Ecuador, Guatemala, Guyana, and Peru all took the position that the due diligence principle is a

[28] United Nations, General Assembly, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, A/76/136 (13 July 2021) p. 48, available at https://undocs.org/en/A/76/136.

[29] "Open-Ended Working Group – UNODA," https://www.un.org/disarmament/open-ended-working-group/ [Accessed February 4, 2022], France's response to the pre-draft report from the OEWG Chair p. 3.

[30] Ibid. Comments submitted by the Czech Republic p. 3.

[31] Supra note 27 p. 26.

[32] Ibid. p. 33.

[33] Ibid. p. 71.

[34] Ibid. p. 76.

[35] Ibid. p. 91.

[36] "Finland Published Its Positions on Public International Law in Cyberspace," https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace [Accessed February 4, 2022].

[37] "Australia's Position on How International Law Applies to State Conduct in Cyberspace." Annex B, https://www.internationalcybertech.gov.au/our-work/annexes/annex-b [Accessed February 4, 2022].

[38] Supra note 28, Republic of Korea Comments on the pre-draft of the OEWG Report p. 5.

[39] "Declaration by the High Representative Josep Borrell, on Behalf of the European Union, on Malicious Cyber Activities Exploiting the Coronavirus Pandemic," https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/ [Accessed February 4, 2022].

[40] "Recommendation CM/Rec(2011)8 of the Committee of Ministers to Member States on the Protection and Promotion of the Universality, Integrity and Openness of the Internet," https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f8 [Accessed February 4, 2022].

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

part of the international law that States must apply in cyberspace."[41] All this practice certainly provides a considerable value for the discussion. After analysing all this practice, it might be constituted that State practice, in favour, is geographically diverse, consistent, and uniform, also, it avoids vague language. Moreover, it should be mentioned that States like France, Australia, the Republic of Korea, Japan, Estonia, the Netherlands, and Germany are among the most relevant states in the cyber domain. It is fair to say, that the concept has a substantial support in international community.

II. State practice opposed to the concept binding nature

There are some States which question the binding nature of due diligence obligation. New Zealand position is: "New Zealand is not yet convinced that a cyber-specific "due diligence" obligation has crystallised in international law."[42] US position is: "The United States has not identified the State practice and opinio juris that would support a claim that due diligence currently constitutes a general obligation under international law."[43] Similar statement was made on behalf of Israel: "we have not seen widespread State practice beyond this type of voluntary cooperation, and certainly not practice grounded in some overarching opinio juris, which would be indispensable for a customary rule of due diligence, or something similar to that, to form."[44] There is some logic why States might not want to be committed to the concept. As Antonio Coco and Talita de Souza Dias provide: "[f]or instance, states may fear that a fine-grained due diligence standard for cyberspace would be too burdensome to implement and could stifle its necessary flexibility."[45] This fear is reasonable, however, the problem is not the concept itself, but rather still the vague application of it. However, as Tomohiro Mikanagi correctly said, "the absence of its clearly defined outer limit cannot deny the existence of the core content."[46] And even though these States challenge the binding nature of the concept, they do not reject it, in addition, these States are not persistent objectors of the concept. Moreover, few States should not exclude concept applicability, especially when they do not object possibility of its applicability. Accordingly, it could be said that there is no practice that would at all reject the

[41] Improving transparency: International law and state cyber operations – Fifth Report (presented by professor Duncan B. Hollis) available at: https://www.oas.org/en/sla/iajc/docs/themes_recently_concluded_International_law_State_cyber_operations_FINAL_REPORT.pdf

[42] "The Application of International Law to State Activity in Cyberspace," https://dpmc.govt.nz/publications/application-international-law-state-activity-cyberspace, 17, [Accessed February 4, 2022].

[43] Supra note 27 p. 141.

[44] "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations." EJIL Talk, https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/ [Accessed February 8].

[45] Coco and Dias p. 783.

[46] Tomohiro Mikanagi, "Application of the Due Diligence: Principle to Cyber Operations," *International Law Studies Series, US Naval War College*, 97 (2021): 1019-1038, p. 1032.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

concept and questioning its applicability due to application questions is reasonable, but per se, it should not mean rejection of the concept applicability.

III. Case law supporting the due diligence binding nature and applicability

One should recall the ICJ position in Corfu Channel and Pulp Mills cases: in those cases, ICJ referred to due diligence as a general concept applicable under international law.[47] In Corfu Channel, it was stated that: "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[48] Permanent Court of Arbitration in Island of Palmas case explicitly stated: "Territorial sovereignty, as has already been said, 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."[49] ICJ dictum in Teheran Hostages case also referred to due diligence, although not in direct language and also in that case, certain protective obligations for Iran were imposed by treaties in force, however, this practice also contributes in proving that due diligence is generally accepted obligation.[50] Similarly as in Hostages case ICJ referred to due diligence in *Bosnian* case also.[51] There was an analysis of diligent behaviour in Nicaragua case.[52] Thus, it is clear – a concept already exists under international law and is not necessarily linked to any specific regime (although its precise application is determined by a specific regime in which it is applied), instead it is linked with sovereignty. And even if there is no specific court practice in the cyber realm - general practice should be accepted.

ICJ provided in Nuclear Weapons advisory opinion – the novelty of weapon should not mean that rules which were created earlier do not apply thus, it does not mean that if new means of war emerged after the creation of rules, those new means are not subject to existing law.[53] Applying this logic and combining it with the fact that due diligence applies as a general rule which regulates behaviour under international law it could be firmly stated that there is no need of proving due diligence concept binding nature, particularly in the cyber domain as the cyber domain is governed by international law and thus, due diligence concept is per se applicable. As due diligence regulates States behaviour, and the use of weapons or new technology is the concern, not the technology (such line of argumentation is also supported by the OEWG report: "it is the misuse of such technologies, not the technologies themselves, that is of concern."),[54] it

[47] Corfu p. 22; Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, I.C.J. Reports 2010, p. 14 101.

[48] Corfu p. 22.

[49] Island of Palmas p. 839.

[50] Teheran Hostages 56-68.

[51] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), 2007 I.C.J. 43 430 [Bosnian Genocide].

[52] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 14. 157 [Nicaragua].

[53] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226, 39; 86.

[54] United Nations *Final Substantive Report* A/AC.290/2021/ CRP.2 (March 2021) 23.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

could be stated that due diligence concept applies because it simply regulates how States should behave when new ways of how to harm are created.

IV. Scholars‘ position

Probably most notable academic work on the subject is Tallinn Manual 2.0. Rule 6 provides an obligation to "exercise due diligence."[55] Some important and valuable explanations could be found in scholars' work. Recently Antonio Coco and Talita de Souza Dias provided an opinion that cyberspace is not a "duty-free zone", and that protective obligation exists irrespective of how the due diligence concept is labelled.[56] The position that due diligence applies under general international law and that international law governs the cyber realm was adopted by Eric Talbot Jensen and Sean Watts.[57] Such opinion corresponds to the case law analysis provided above. Michael N. Schmitt supports the view that sovereignty has a corresponding obligation of due diligence.[58] Authors Scott J. Shackelford, Scott Russell, and Andreas Kuehn provide that principle envisaged in Corfu "carries over" to the cyber realm.[59] Considering that all these mentioned authors are well known for their research of cyber issues also that their position corresponds to the concepts established by case law it should be clear that concept is applicable.

Conclusion

After currently existing State practice analysis, one could see clear support for the binding nature of the concept. Even though a number of States remain silent, it should not be necessary for all the States to provide their opinion. Moreover, as due diligence exists under general international law and comes from the principle of sovereignty, there should be no question if due diligence is applicable. Not only relevant States express their positive view on the matter but also prominent academics. Hence, it may be stated that the due diligence concept is applicable in the cyber domain, however, how it applies and could it solve the problem of attribution will be covered in the following section.

[55] Tallinn Manual Rule 6.

[56] Coco and Dias p. 783.

[57] Eric Talbot Jensen, Sean Watts, "Cyber Due Diligence," *Oklahoma Law Review* 73, no. 4 (Summer 2021): 645-710 p. 692.

[58] Michael N. Schmitt, "In Defense of Due Diligence in Cyberspace," *Yale Law Journal Forum* 125 (2015-2016): 68-81, p. 80.

[59] Scott J. Shackelford, Scott Russell, Andreas Kuehn, (2016) "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors," *Chicago Journal of International Law*: Vol. 17: No. 1, Article 1, p. 8.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

DUE DILIGENCE CONCEPT APPLICATION AND ANALYSIS OF HOW IT MIGHT (IF AT ALL) CONTRIBUTE TO SOLVING THE ATTRIBUTION PROBLEM

Due diligence concept might be hard to describe, and even if it is described in an exact set of behaviour rules or standards, they are mainly regime based and are variable depending on activity.[60] As Eric Talbot Jensen and Sean Watts tell about the essence of cyber due diligence: "[t]he precise standards of conduct and result that follow from the principle and its doctrine remain unclear."[61] When there is such legal uncertainty, it is hard to constitute if a State has violated this rule or not. Nevertheless, after reviewing case law on the issue, scholars' work, and recent State practice, one could say that certain rules on how and when to establish State responsibility based on due diligence violation do exist, even though there are no firmly established domain-specific rules. However, it does not mean that due diligence has no developments in the cyber domain. To analyse of how (if) due diligence may contribute to solving the attribution problem and thus responsibility issue, it should be understood what due diligence essence is, how it applies under general international law, and then look what are the main due diligence ideas in the cyber context. In this section, it will be first looked at how due diligence is understood in general terms, what conditions establishment or non-fulfilment by a State may lead to State responsibility, then it will be looked how, if at all, this rule can work in practice.

Conditions of cyber due diligence overview

First, it is necessary to highlight that the rule is regarded as an obligation of means, not of the result.[62] This may automatically presume that not in every case state may be held responsible for failure to ensure. A general definition of due diligence could be found in the very first judgment of ICJ: "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[63] This is where the simplicity ends. It is accepted that how exactly due diligence applies is still a subject of debate.[64]

To understand when a State violates due diligence, it is wise to recall ICJ practice. From the *Corfu Chanel* case, one could draw such conclusions – first, the act should be made in its (State) territory, or under its control. Secondly, there should be knowledge of such conduct. And finally, the act should be contrary to the rights of other States. Regarding the knowledge criteria, Court, in this case, also referred to circumstantial evidence on determining if Albania knew about mine

[60] Responsibilities and obligations of States with respect to activities in the Area, Advisory Opinion, 1 February 2011, ITLOS Reports 2011, p. 10 117; Heike Krieger, Anne Peters, Leonhard Kreuzer, and Eric Talbot Jensen, "Due Diligence in Cyber Activities." Essay in *Due Diligence in the International Legal Order*, 252–69, (Oxford, United Kingdom: Oxford University Press, 2020), p. 253, **[Jensen]**.

[61] Supra note 57 p. 702.

[62] Bosnian Genocide 430.

[63] Corfu p. 22.

[64] Jensen p. 254.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

lying activity. Thus, the rule of circumstantial evidence for (constructive) knowledge fact establishment (which will be useful for further analysis) might also be drawn from this case. In the Teheran Hostages case ICJ referred to 4 elements – awareness of the obligation to protect, awareness (or knowledge) of a need of help (or to stop illegal activity), means to fulfil the protection obligation, and failure to do it.[65] In this case Court referred to State ability to fulfil the obligation, and when applying such condition to the cyber realm it might be seen that clearly some States do not have the same capacity and ability as some major cyber players, due to this due diligence might not only depend on a specific domain, but also on each specific State capacity.[66] In the Bosnian Genocide case ICJ stipulated the "capacity to influence effectively" the actor who is behind the conduct, criteria.[67] In the Nicaragua case Court put much emphasis on State capacity to prevent (or ability) criteria.[68] The Same position was of Judge Alvarez in Corfu case.[69] Thus, one can see that at least ICJ position on this obligation (under general international law) is quite well established.

Scholars who analyse or develop cyber norms also provide their understanding of how due diligence applies and what are the preconditions for its application in the cyber domain. Tallinn Manual authors' position is that: "[a] State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States."[70] Later Manual authors discuss and analyse same criteria as stipulated by ICJ, territory, knowledge, capacity, and harm, although with harm, what is interesting, Manual authors use the wording 'serious adverse consequences' and such position might be disputed as it will be seen bellow. Delerue for cyber due diligence definition also uses the dictum from the Corfu Channel case.[71] Jensen and Watts write: "due diligence requires States to not knowingly allow their territory be a source of transboundary harm."[72] Hence, it could be constituted that definition provided by ICJ case law is suitable.

Recently, there have also been some so needed developments in State practice on due diligence application, although these opinions or positions provided by States are not as comprehensive and widely expressed as desired. An important joint position of States is expressed in the latest report of GGE.[73] There are 4 points addressed – knowledge, territory, reasonable and feasible steps. Interestingly, this report instead of an act contrary to the rights of other states formulation used internationally wrongful act wording, which automatically presumes that a certain threshold (and a pretty high one) of harm should be reached, as not every act is considered as wrongful, no further guidance was provided. In general, it may be said that the 2021 GGE report at least provides more guidance on the norm application compared to 2015

[65] Teheran Hostages 68.
[66] Supra note 57 p. 75.
[67] Bosnian Genocide 430.
[68] Nicaragua 157.
[69] Supra note 18 Judge Alvarez separate opinion p. 44.
[70] Tallinn Manual Rule 6.
[71] Delerue p. 356.
[72] Supra note 56 p. 691.
[73] Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc. A/76/135 (14 July 2021), 29-30.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

report, although it does not elaborate on each criterion in more detail, and thus there is still room for improvement and development.

Regarding individual State practice, the Netherland's position is "that the due diligence principle applies only if the State who's right or rights have been violated suffers sufficiently serious adverse consequences."[74] Also, the Netherlands referred to other conditions – knowledge fact, and control of ICT's. Japan, on its behalf, says that the factors like "the seriousness of the cyber operations in question and the capacity of the territorial States to influence a person or group of persons conducting the attacks" should be taken into account.[75] Estonia, for instance, emphasized capacity and ability of a State.[76] The Czech Republic on its behalf does not go far from standard formulation, however, puts emphasis on State capacity.[77] New Zealand which objects the fact that due diligence is a binding obligation in the cyber domain, provides a view that if due diligence would be of binding nature, then "it should apply only where states have actual, rather than constructive, knowledge of the malicious activity, and should only require states to take reasonable steps within their capacity to bring the activity to an end."[78] However, such position contradicts the ICJ practice from the Corfu Channel case, though, not necessarily wrongly, however, this is a minority position. From individual State practice, such conclusion can be made: different States have slightly different positions on how due diligence applies (though it is more related to the application of the criteria not the criteria itself), moreover, individual declarations are not widespread, and this is the biggest struggle for norm development. Therefore, without further cooperation between States, and an attempt to reach consensus it will remain ambiguous.

After analysing ICJ case law, scholars' position, and State practice, which is yet underdeveloped, still it might be constituted that State violates this norm when: an act emerges from the territory (or ICT's) under its control, when there is knowledge of such activity, when a State is capable to stop such conduct and when the act is contrary to the rights of target State.

Analysis of how due diligence based responsibility can practically work

Now, when due diligence essence in the cyber realm is described, at least to the extent currently possible, the question is how it might work with cyber-attacks conducted by proxies. In this section, it will be analysed how State responsibility for due diligence obligation violation when proxies are used can be established by going through each condition and practically applying it. Although such application of due diligence might not correspond to the original idea of it, however, one can see that even ICJ supports the possibility of such application of due diligence when other responsibility mechanisms, in particular, attribution, fail. For instance, in both *Bosnian* and *Teheran Hostages* cases, ICJ first went through attribution rules, and once it was established that there were no sufficient grounds to attribute acts to States, the Court then

[74] Supra note 27 p. 59.
[75] Ibid. p 48.
[76] Ibid. p. 26.
[77] Supra note 28, p. 3.
[78] Supra note 41.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

moved to due diligence violation evaluation. In this way, the Court tried to find a way to avoid impunity for wrongful acts, which under established rules were impossible to attribute to a particular State. Thus, such application of due diligence obligation is not a new approach. Such view of due diligence application is also supported by Martin Ney and Andreas Zimmermann, they provide: "[n]o matter how this principle is labelled, [referring to the due diligence] it is of particular relevance in cases where harmful actions either cannot be attributed to a particular State or where only insufficient proof for such attribution can be provided by the victim State."[79] Christian Walter tells that this principle "extend the responsibility of States for private action beyond the strict criteria of Article 8."[80] Scott J. Shackelford and Richard B. Andres calls it "governmental awareness" test which may apply when there is not enough evidence for traditional attribution ways.[81] Other scholars also support the idea that due diligence obligation might help to answer the attribution problem.[82] What is necessary to mention, in such a case State is not responsible for the act itself (as the original perpetrator) but rather for its failure to ensure that such actions will not happen (the failure to ensure).[83] As Michael N. Schmitt writes:

"If the territorial state fails to terminate an ongoing non-state cyber operation mounted from its territory against another state, and doing so is practical and reasonable in the circumstances, then the territorial state commits an internationally wrongful act by failing to exercise its obligations under the principle."[84]

Nevertheless, such responsibility still brings accountability and does not allow to escape responsibility by hiding under proxies. However, if such a mechanism of responsibility is feasible and practically possible, it will be analysed in the following paragraphs.

I. Territory condition application

Regarding the territory, in 2015 UN GGE report, it is stated – "States have jurisdiction over the ICT infrastructure located within their territory."[85] Under Tallinn Manual Rule 1, "States enjoy sovereignty over any cyber infrastructure located on their territory and activities associated with that cyber infrastructure."[86] Jensen provides that "the assertion of jurisdiction over ICTs by states reciprocally implies that states must also exercise control over those

[79] Martin Ney, Andreas Zimmermann, "Cyber-Security beyond the Military Perspective: International Law, Cyberspace, and the Concept of Due Diligence," *German Yearbook of International Law* 58 (2015): 51-66, p. 62.

[80] Christian Walter, "Obligations of States, before, during, and after a Cyber Security Incident," *German Yearbook of International Law* 58 (2015): 67-86, p. 74.

[81] Scott J. Shackelford, Richard B. Andres, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem," *Georgetown Journal of International Law* 42, no. 4 (2011): 971-1016, p. 989.

[82] Eric Talbot Jensen, Sean Watts, "A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?" 95 *Texas Law Review* 1555 (2017), p. 1558; Jensen p. 263-264; Luke Chricop, "A Due Diligence Standard of Attribution in Cyberspace," *International and Comparative Law Quarterly* 67, no. 3 (July 2018): 643-668 p. 651 **[Chricop]**; Delerue p. 356.

[83] See e.g., Bosnian Genocide 430.

[84] Supra note 57 p. 79.

[85] GGE 2015 Report 28(a).

[86] Tallinn Manual Rule 1 commentary 1.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

ICTs."[87] As was discussed in the previous section, due diligence applies in the cyber domain. States have a general obligation of due diligence, which comes from sovereignty, and as States enjoy sovereignty over their cyber infrastructure, States have an obligation not to allow it knowingly to be used for malicious acts against other States. Importantly, Robert Kolb provides that the control over ICT's is rather a question of fact, not the law.[88] Therefore, it may be constituted that once it is established that a cyberattack occurred from cyberinfrastructure in a particular State, which can be proved via technical evidence, the territory requirement is established (though complex issue to find the original perpetrator may arise in case one State uses other State's infrastructure to route the attack). For example, regarding the attacks made by UNC1151 (*Ghostwriter)*[89], the Mandiant report provided that "[s]ensitive technical information locates the operation in Minsk."[90] What exact information is this might not be disclosed in order not to reveal perpetrators vulnerabilities, however, it is true that by using technology the geolocation of attacks can be traced, even though, not necessarily easy. If such proof would be sufficient, it is for a Court to deliberate. However, it will be based on technical evidence, and there is a high probability that the attack can be traced accurately; as mentioned, it is the question of fact, not the law. It is true that the risk of other State involvement, and this is the reason why territory criteria shall not be looked isolated, rather is should be closely related with knowledge criteria in order to avoid situations where State is held responsible for cyber-attacks which where routed through its territory without any or very minimal possibility to know it. In fact, the possibility to route the attacks should encourage every State to take certain precautionary measures in order to avoid responsibility for other unfriendly States' acts.

II. Knowledge fact establishment

Knowledge fact establishment might be the hardest part and, at the same time, the most important aspect of due diligence. Once knowledge fact is established, it might be extremely hard for a State to defend itself from due diligence violation allegations. Necessary to mention that knowledge fact establishment does not depend on the proximity of the conduct but rather on the State possession of the information.[91] Such a view is based on ICJ position from the *Bosnian Genocide* case.[92] Thus, once again it is the question of fact, however, the criterion how to say that

[87] Jensen p. 257.

[88] Robert Kolb, "Reflections on Due Diligence Duties and Cyberspace," *German Yearbook of International Law* 58 (2015): 113-128 p. 120.

[89] Ghostwriter operation is both hacking and disinformation operation (main goal of the operation is to sway elections, disrupt local political ecosystems, and create distrust of US and NATO forces). Its' mainly targets were NATO (Eastern-flank) and EU countries (variety of governmental and private sector entities), it is considered that Ghostwriter was conducted by State-sponsored UNC1151 group.

[90] UNC1151 Assessed with High Confidence to Have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests," Mandiant; https://www.mandiant.com/resources/unc1151-linked-to-belarus-government?fbclid=IwAR00rft8HJd0aQ1SmUzKsfL7_f1VoB7D5CgNvsuEayVNY3G1rPm6v-Z6KMk [Accessed January 18, 2022].

[91] Coco and Dias.

[92] Bosnian Genocide 436.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

the State has possessed information or had knowledge is a legal question. Knowledge can be direct (e.g., notification by a target State),[93] or there can be constructive knowledge (State should "normally be aware" of act happening).[94] Tallinn Manual authors as well refers to "constructive knowledge."[95] As Luke Chricop provides: "[w]hilst it might be difficult to ascertain evidence of a State's actual knowledge of a given cyber operation, a constructive knowledge standard ensures that the due diligence approach is not rendered all but redundant."[96] This constructive knowledge possibility in the due diligence norm is crucially important in the cyber domain. For instance, in environmental law, it is normal to require a State to constantly monitor the activities happening under its jurisdiction.[97] In the cyber domain, such mass surveillance might be called a "Trojan horse" for civil liberties, as Karine Bannelier-Christakis said.[98] Thus, constant monitoring might not be possible nor feasible, or even legal, apart from victim State notification, there is a low chance that direct knowledge could be established and therefore, this constructive knowledge possibility is essential.

Nevertheless, this constructive knowledge possibility does not mean that it is easy to prove the knowledge fact. As it was stated in Corfu case: "it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein, nor yet that it necessarily knew, or should have known, the authors."[99] For example, in The South China Sea Arbitration court supported the idea that it is unreasonable to expect from a State that it will be always able to know when its individuals who are affecting other State territory and prevent (although in this case harm was done from a vessel flying a State flag).[100] Later in evaluation by Court in that case, it was showed, that some official China government vessels accompanied the ships and from this fact it was constituted that China ought to know about illegal activity.[101] Tallinn Manual take on constructive knowledge criteria is that it should be based on the objectiveness.[102] Therefore, even if the law provides a possibility of constructive knowledge application, there is still a procedural issue to prove it and as Delerue writes it is up to victim State to prove that the territorial State should have known about the conduct.[103]

This constructive knowledge can be based on circumstantial evidence.[104] As mentioned in the first part of this article, cyber-attacks are covered by the shield of high secrecy, and this is where the concept of circumstantial evidence highlighted by ICJ in Corfu judgment becomes essential. As highlighted by the Court, "[s]tate should be allowed a more liberal recourse to

[93] Tallinn Manual Rule 6 commentary 37.
[94] Bosnian Genocide 432.
[95] Supra Note 69 39.
[96] Chricop p. 650.
[97] Pulp Mills 197.
[98] Karine Bannelier-Christakis, "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?" *Baltic Yearbook of International Law Online* 14, no. 1 (2015): 23–39, p. 31.
[99] Corfu p. 18
[100] South China Sea Arbitration, Philippines v China, Award, PCA Case No 2013-19, ICGJ 495 (PCA 2016), 12th July 2016, Permanent Court of Arbitration 754.
[101] Ibid. 755.
[102] Supra note 92.
[103] Delerue p. 366.
[104] Corfu p. 18.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

inferences of fact and circumstantial evidence,"[105] and this should be allowed in cases where the victim State might not be able to collect necessary evidence.[106] This might be precisely a case in the cyber domain, where without any illegal collection of evidence it might be extremely difficult to obtain direct evidence. Thus, it might be said that knowledge fact can be proved via circumstantial evidence. However, those evidence should allow objectively prove it as provided in Tallinn Manual and should lead "to a single logical conclusion." Once again, how to determine if circumstances prove the knowledge is not so clear. It could be only tried to look at it through a practical example.

Applying these rules practically, the UNC1151 actor again may serve as an example. From Mandiant report, such factual circumstances might be drawn targets of this UNC1151 were the opposition of Belarus government, other States ministries of defence were targets, overall targeted States had complicated bilateral relationship with Belarus government.[107] Operations performed by actor gave no monetary value, thus someone needed to finance it, also, such operations are not cheap, especially when they last in time. If it could be presumed that actors were, in fact, working back-to-back with authorities, then it would put Belarus in the same position as China was put in South China Sea Arbitration case. Maybe such circumstances cannot clearly constitute knowledge fact for legal purposes, but as Tallinn Manual provide:

"[i]f particular cyber infrastructure has been repeatedly exploited for the purposes of conducting harmful cyber operations against other States, it may be reasonable to conclude that it will be so used again. Similarly, if a particular group has repeatedly mounted such operations, it may be highly likely that the group will do so in the future."[108]

It is known that this UNC1151 actor is responsible for a series of cyber-attacks and operations, operations are lasting in time, and some States have raised concerns and even accused Belarus: there is a credible report by Mandiant which says that Belarus is responsible.[109] Recently, there was a report by Ukrainian officials that this same group is probably behind the recent cyber-attacks against Ukraine, authorities reasoned it by the similarity of the script (and from technical part it is quite an important evidence).[110] All this can reasonably indicate that Belarus at least should know about such a group operating from its territory (to hold that group a proxy in a legal sense more evidence might be needed), and thus Belarus should have known about a high risk of new attacks, thus higher degree of care should be performed. Nevertheless, gathering necessary evidence is also not an easy task, though much simpler than proving control or instructions. Still, there might not be complete certainty, and some assumptions will be needed.

[105] Ibid.
[106] Supra note 97 p. 29.
[107] Supra note 89.
[108] Tallinn Manual Rule 7 commentary 14.
[109] "EU Formally Blames Russia for Ghostwriter Influence Operation," https://therecord.media/eu-formally-blames-russia-for-ghostwriter-hack-and-influence-operation/ [Accessed January 17, 2022]; Supra note 89.
[110] "CERT-UA," https://cert.gov.ua/article/38155, [Accessed April 9, 2022].

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

III. Harm threshold

Harm criteria might be the most disputed criteria of due diligence, although not the existence itself, but rather its essence. Tallinn Manual authors see "serious adverse consequences" as one of the preconditions for due diligence invocation. Manual authors hold that a certain threshold of harm must be reached. However, from the commentary to article 6, it is unclear what exact degree of harm would be sufficient, there is only a brief guidance. In summary of commentary to article 6, it might be said that according to authors, due diligence could only be invoked where there is an internationally wrongful act conducted or if it is a case with non-States actors: "the due diligence obligation only attaches when a non-State actor engages in conduct that affects a right of the target State, that is, the conduct would, if conducted by the territorial State, breach an obligation that State owes the target State."[111] However, this serious consequences criteria is not supported by all scholars. Delerue argues, "I am not convinced that such requirement of a threshold of harm is part of the customary principle of due diligence, and thus of the lex lata applicable to cyber operations."[112] Such opposition might be substantiated. One of the possible drawbacks of this *"serious adverse consequences"* criteria is that if, for example, there are more than one cyber interference, which if looked isolated does not reach the necessary harm threshold but if a couple of such interferences are compounded and result in certain severe violation (e. g., long term election interference),[113] then there is a risk that for neither of each such minor interference (even considered in concert) due diligence will be applied and territorial State might reach its goals without being responsible. A similar scenario was analysed by the authors of the Tallinn Manual. In fact, as disclosed in a commentary, the authors were split on this, while the minority of them suggested: "the individual operations may be treated as a composite armed attack if conducted by the same originator or by originators acting in concert,"[114] the majority was in the position that "aggregation is inappropriate."[115] Thus, this is one of the biggest critiques for Tallinn Manual as States for some very severe cyber operations which are conducted in episodes for long term might remain imputable. Coco and Dias were also not convinced that a threshold of harm exists (although they do concede that States should not be responsible for negligible disruptions),[116] their position was rather that this threshold is borrowed from a different 'no-harm' obligation.[117] Even if it could be agreed at least to a certain extent (as some new state practice also supports this[118]) on *serious harm* condition which is transferred from environmental law,[119] the rejection of aggregation of more minor cyber interferences which cumulatively can cause serious consequences is clearly disputable. In cyber realm the aggregation concept could be taken from jus ad bellum. Usually the minor harm incidents are way how persistent threat actors work, they gather certain information for long time form different channels by accessing

[111] Tallinn Manual Rule 6 commentary 22.
[112] Delerue p. 365.
[113] See Coco and Dias p. 787.
[114] Tallinn Manual Rule 6 commentary 30.
[115] Ibid. 31.
[116] Coco and Dias p. 786.
[117] Ibid.
[118] Supra note 27.
[119] Delerue p. 364.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

them without authorization, and this information might be used to cause several separate attacks, which might not necessarily reach a required level of harm, but if taken in concert it might constitute a major violation of international law norms.

IV. Capacity evaluation

The capacity of each State is also a critical condition of due diligence. This element is directly related to the nature of the due diligence – the obligation of means, not the result. It is accepted among scholars and case law that it should not be demanded from a State more than it can do, considering its level of development and means available to it. Michael N. Schmitt provides that: "the due diligence obligation does not require a state to take measures that are beyond its means or otherwise unreasonable."[120] Robert Kolb states: "[n]o State is obliged to do the impossible and none is obliged to venture into the unreasonable."[121] Judge Alvarez in the Corfu Chanel case provided that "[p]ower is not obliged to exercise greater vigilance than is consistent with the means at its disposal."[122] ICJ in Nicaragua case emphasised State ability and heavily referred to the resources available to that country.[123] In Bosnian Genocide case ICJ in the direct words said: "employ all means reasonably available to them."[124] As it was provided by ICSID: "the standard of due diligence is that of a host state in the circumstances and with the resources of the state in question."[125] Automatically question arises how to determine if a State is cyber capable? What are the criteria.

As Tallinn Manual commentary provides: "[t]he feasibility of particular measures is always contextual. The developed States will often be more capable of stopping harmful cyber operations that emanate from their territory than developing States."[126] Maybe such capacity could be proven via some cyber-capabilities rating?[127] Or maybe IT sector development might be a factor to consider? Further, the manual authors provide: "[f]easibility depends, inter alia, on the technical wherewithal of the State concerned, the intellectual and financial resources at its disposal, the State's institutional capacity to take measures, and the extent of its control over cyber infrastructure located on its territory."[128] Thus, some abstract criteria are provided but what is the threshold for each it is not clear. One possibility of how State capacity could be shown is via how previously the State has reacted to similar accidents. Such a conclusion could be drawn from

[120] Supra note 57 p. 80.
[121] Supra note 87 p. 123.
[122] Supra note 68.
[123] Nicaragua 157.
[124] Bosnian Genocide 430.
[125] Pantechniki SA Contractors and Engineers v Albania, Award, ICSID Case No ARB/07/21, IIC 383 (2009), 28th July 2009 81.
[126] Tallinn Manual Rule 7 commentary 16.
[127] For instance: "Cyber Capabilities and National Power: A Net Assessment," https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power, [Accessed April 9, 2022].
[128] Supra note 125.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

the ICJ argumentation in the Teheran Hostages case.[129] From the Armed Activities case it could be said that if a State tolerates hostile groups and has a real ability to put an end to their activities, it may be considered in breach of the duty of vigilance. Regarding State practice, there is only a miserable amount of it on the capacity element. Estonia provides that "technical, political and legal capacities of a state" shall be considered.[130] Japan makes a reference to the capacity to influence criteria.[131] Thus, it is clear, broader, and more comprehensive State practice and criteria development is needed. Nevertheless, the level of State development, attitude to incidents, and previous experience might be the factors to consider.

Although generally capacity is proven by objective data, the criteria how to determine what is a cyber developed State and what is not, when to say that a state is cyber capable is a legal question, and apparently, there is no clear answer to date, only some ideas. Precise criteria establishment is crucial. There is also a possibility of "capacity to influence" criteria developed by ICJ in the *Bosnian Genocide* case. If the ability to influence could be proved, then the State shall be considered as having the capacity to stop such attack. In the Bosnian Genocide case, ICJ provided: "capacity itself depends, among other things, on the geographical distance of the State concerned from the scene of the events, and on the strength of the political links, as well as links of all other kinds, between the authorities of that State and the main actors in the events."[132] Court did not put *numerus clausus* of links that could prove such capacity, which should presume that the Court is liberal on this question. The ICJ provides a generous leeway for link establishment, however, in the end, it once again relates to the facts which need to be established, and thus, some minimum evidence will be required, although indeed, the same standard of proof as in attribution mechanisms should not be needed; otherwise, the idea of due diligence would be meaningless as then State could easily prove attribution on the instructions concept.

Conclusion

How exactly due diligence applies in a cyber domain such findings can be made. Firstly, if the cyberinfrastructure of a State was used, then the criterion of the territory is fulfilled. Secondly, if it is proved that State had at least constructive knowledge about cyber-attack, then the knowledge criterion is fulfilled; however, this depends on factual circumstances, and more clarifications or consensus among the States is needed, still more liberal approach is supported. Thirdly, there is no mutual agreement on the harm criterion, and scholars are divided; States do not provide exact answers to what harm could suffice to apply the principle; thus, it remains one of the most disputed criteria. Nevertheless, cyber-attacks that violate established rights of other State will suffice, but it is not an issue (provided, that aggregation currently might not be acceptable) considering how cyber-attacks are conducted now (mostly by launching numerous minor attacks with common goal to make impact for particular State). Regarding the capacity criterion, there are two findings. One relates to the technological development of a State, which purely depends on facts that are objective, still exact criteria what is a cyber-developed State

[129] Armed Activities in the Territory of the Congo (Democratic Republic of the Congo v Uganda) [2005] ICJ Rep 168 300-301.
[130] Supra note 27 p. 26.
[131] Supra note 27 p. 48.
[132] Bosnian Genocide 430.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

needs to be established. Another depends on a more subjective criterion – the capacity to influence. On either of each, the capacity criterion could be established. Finally, with respect to the evidence questions, and unreasonably high standard of proof, it could be said that with respect to due diligence, a more liberal approach could be applied. If doctrine with respect to attribution and evidence is rigorous, then regarding due diligence, one could see that approach even taken by ICJ is more liberal, mainly because not the question of the attributability is decided but rather the question of a violation of a duty to ensure due diligence, however, in the end it still results in State responsibility. Indeed, the doctrine is still complicated and ambiguous. However, with more State practice, it could be developed, and ambiguities may be answered. Undoubtedly, applying this doctrine is much simpler than establishing attribution. Yet, more developments are needed to shape clear rules and criteria.

CONCLUSION

1. As shown, cyber due diligence is still in the development phase (the essence of how it applies), and more cooperation between States is necessary. One could see that quite a few key questions still need to be answered, like the essence of harm or capacity criteria. The following recommendation could be made - States should agree to draft a legal document with binding rules dedicated to international cyber law together with their detailed explanation. Nevertheless, it is doubtful whether such document should be a treaty, as, under international law, some crucial issues which were attempted to be regulated under treaty law failed because some States which engages the most in particular activities were reluctant to ratify or join to such treaties, and thus the treaty regulation had not fulfilled its purpose. Probably, codification should be awarded to ILC, and ILC can follow the example of ARSIWA where specific rules were codified, however, they never became treaty law but still are binding upon States due to their broad endorsement. This could help to crystalize cyber norms, including the application of due diligence, and bring more clarity into the underdeveloped and vague legal domain.
2. It still could be constituted that due diligence is one of the key answers to the responsibility issue concerning proxies' conduct. Even though more development is needed and questions to be answered, it still can help establish accountability in the cyber domain due to more liberal application.

LEGAL REFERENCES

Books

1. Delerue, François. Cyber Operations and International Law. Cambridge Studies in International and Comparative Law. Cambridge: Cambridge University Press, 2020.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

2. Heike Krieger. Peters Anne. Kreuzer Leonhard, and Jensen Eric Talbot. “Due Diligence in Cyber Activities.” Essay. In *Due Diligence in the International Legal Order*, 252–69, p. 253. Oxford, United Kingdom: Oxford University Press, 2020.

Special literature

3. Bannelier-Christakis. Karine. “Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?” *Baltic Yearbook of International Law Online* 14. No. 1 (2015): 23–39.
4. Broeders. Dennis. De Busser. Els and Pawlak. Patryk. “Three Tales of Attribution in Cyberspace: Criminal Law, International Law and Policy Debates.” (April 1, 2020). *The Hague Program for Cyber Norms Policy Brief*. 2020.
5. Chricop. Luke. "A Due Diligence Standard of Attribution in Cyberspace." *International and Comparative Law Quarterly* 67. No. 3 (July 2018): 643-668.
6. Coco. Antonio. Talita de Souza. Dias. “‘Cyber Due Diligence’: A Patchwork of Protective Obligations in International Law.” *European Journal of International Law* 32. no. 3 (2021): 771–806.
7. Eichensehr. Kristen E. "Cyberwar & International Law Step Zero." *Texas International Law Journal* 50. no. 2-3 (Spring-Summer 2015): 357-380.
8. Finlay. Lorraine. and Christian. Payne. “The Attribution Problem and Cyber Armed Attacks.” *AJIL Unbound* 113 (2019): 202–6.
9. Hathaway. Oona A. Chertoff. Emily. Dominguez Lara. Manfredi. Zachary. Tzeng. Peter. "Ensuring Responsibility: Common Article 1 and State Responsibility for Non-State Actors." *Texas Law Review* 95. no. 3 (February 2017): 539-590.
10. Jensen. Eric Talbot. Watts. Sean. "Cyber Due Diligence." *Oklahoma Law Review* 73. no. 4 (Summer 2021): 645-710.
11. Jensen. Eric Talbot. Watts. Sean. “A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?” 95 *Texas Law Review* 1555 (2017).
12. Katagiri. Nori. “Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks.” *Journal of Cybersecurity* 7. no. 1 (2021).
13. Kolb. Robert. "Reflections on Due Diligence Duties and Cyberspace." *German Yearbook of International Law* 58 (2015): 113-128.
14. 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* 21. no 3. Winter 2016: Pages 405–428.
15. Mikanagi. Tomohiro. "Application of the Due Diligence: Principle to Cyber Operations." *International Law Studies Series. US Naval War College.* 97 (2021): 1019-1038.
16. Ney. Martin. Zimmermann. Andreas. "Cyber-Security beyond the Military Perspective: International Law, Cyberspace, and the Concept of Due Diligence." *German Yearbook of International Law* 58 (2015): 51-66.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

17. Schmitt. Michael N. "In Defense of Due Diligence in Cyberspace." *Yale Law Journal*
Forum 125 (2015-2016): 68-81.
18. Schmitt. Michael N. and Vihul. Liis. “Proxy Wars in Cyber Space: The Evolving International Law of Attribution.” (May 31, 2014). I(II) *Fletcher Security Review* 55-73.
19. Shackelfor. Scott J. Russell. Scott. 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. Article 1.
20. Shackelford. Scott J. Andres. Richard B. "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem." *Georgetown Journal of International Law* 42. no. 4 (2011): 971-1016.
21. Tran. Delbert. “The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack.” 20 *YALE J. L. & TECH.* 50: 376-441.
22. Walter. Christian. "Obligations of States, before, during, and after a Cyber Security Incident." *German Yearbook of International Law* 58 (2015): 67-86.

Legislation

23. International Law Commission Articles on Responsibility of States for Internationally Wrongful Acts. 56th Sess. A/RES/56/83 2002.
24. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. UN Doc. A/76/135 14 July 2021.
25. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. UN Doc A/79/174 22 July 2015.
26. United Nations *Final Substantive Report* A/AC.290/2021/ CRP.2 March 2021.
27. United Nations. General Assembly. *Developments in the field of information and telecommunications in the context of international security: Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266*. A/76/136 13 July 2021. Available at https://undocs.org/en/A/76/136.
28. “Annex B: Australia's Position on How International Law Applies to State Conduct in Cyberspace.” Annex B: Australia's position on how international law applies to State conduct in cyberspace | Australia's International Cyber and Critical Tech Engagement; https://www.internationalcybertech.gov.au/our-work/annexes/annex-b [Accessed February 4, 2022].
29. “The Application of International Law to State Activity in Cyberspace.” The application of international law to state activity in Cyberspace, December 1, 2020.

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

https://dpmc.govt.nz/publications/application-international-law-state-activity-cyberspace. [Accessed February 5, 2022].
30. Finland Published Its Positions on Public International Law in Cyberspace." Valtioneuvosto; https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace [Accessed February 4, 2022].
31. Zaken, Ministerie van Buitenlandse. "Letter to the Parliament on the International Legal Order in Cyberspace." Parliamentary document | Government.nl. Ministerie van Algemene Zaken, September 26, 2019. https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace appendix at 4. [Accessed March 16, 2022].

Case law

32. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro). 2007 I.C.J. 43.
33. Armed Activities in the Territory of the Congo (Democratic Republic of the Congo v Uganda) [2005] ICJ Rep 168.
34. Corfu Channel (United Kingdom v Albania) (Merits) [1949] ICJ Rep 4.
35. Corfu Channel (United Kingdom v Albania) (Merits) [1949] ICJ Rep 4. Judge Alvarez separate opinion.
36. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226.
37. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 14.
38. Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, I.C.J. Reports 2010, p. 14.
39. Island of Palmas Neth. v. U.S. 2 R.I.A.A. 829, (Perm. Ct. Arb. 1928).
40. Pantechniki SA Contractors and Engineers v Albania. Award. ICSID Case No ARB/07/21. IIC 383 2009. 28th July 2009.
41. Responsibilities and obligations of States with respect to activities in the Area. Advisory Opinion. 1 February 2011, ITLOS Reports 2011, p. 10.
42. South China Sea Arbitration, Philippines v China, Award, PCA Case No 2013-19, ICGJ 495 (PCA 2016), 12th July 2016, Permanent Court of Arbitration.

Other references

43. "CERT-UA." cert.gov.ua. https://cert.gov.ua/article/38155. [Accessed February 8, 2022].
44. "Cyber Capabilities and National Power: A Net Assessment." IISS. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power. [Accessed February 20, 2022].
45. "Declaration by the High Representative Josep Borrell, on Behalf of the European Union, on Malicious Cyber Activities Exploiting the Coronavirus Pandemic."

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/. [Accessed January 8, 2022].

46. “Declaration by the High Representative on Behalf of the European Union on Respect for the EU's Democratic Processes.” https://www.consilium.europa.eu/en/press/press-releases/2021/09/24/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-respect-for-the-eu-s-democratic-processes/ [Accessed January 16, 2022].
47. “Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations.” EJIL Talk, December 9, 2020. https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/ [Accessed January 14, 2022].
48. “Office of the Director of National Intelligence A Guide to Cyber Attribution - Dni.gov.” https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf [Accessed January 18, 2022].
49. “U.S. Blames Russia for ‘NotPetya’ Cyber-Aatack.” National Archives and Records Administration. https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/ [Accessed January, 17].
50. “UNC1151 Assessed with High Confidence to Have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests.” Mandiant; https://www.mandiant.com/resources/unc1151-linked-to-belarus-government?fbclid=IwAR00rft8HJd0aQ1SmUzKsfL7_f1VoB7D5CgNvsuEayVNY3G1rPm6v-Z6KMk [Accessed January 18, 2022].
51. Eatwell. T. J. (2020). State Responsibility for the Unlawful Conduct of Armed Groups (Doctoral thesis).
52. Improving transparency: International law and state cyber operations – Fifth Report (presented by professor Duncan B. Hollis) available at: https://www.oas.org/en/sla/iajc/docs/themes_recently_concluded_International_law_State_cyber_operations_FINAL_REPORT.pdf
53. Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: (Cambridge University Press) 2017.
54. Volz. Dustin. “U.S. Blames North Korea for 'WannaCry' Cyber Attack.” Reuters. https://www.reuters.com/article/us-usa-cyber-northkorea-idUSKBN1ED00Q [Accessed January 17, 2022].

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

SANTRAUKA

AR TINKAMO RŪPESTINGUMO KONCEPCIJA GALI PRISIDĖTI PRIE PROBLEMOS, SUSIJUSIOS SU NEVALSTYBINIŲ VEIKĖJŲ, KURIUOS VALSTYBĖS NAUDOJA KAIP MARIONETES, VYKDOMOMS KIBERNETINĖMS ATAKOMS, IŠSPRENDIMO?

Šio darbo tikslas yra išanalizuoti, kur slypi pagrindiniai priskyrimo („attribution“) problemos neveiksmingumo niuansai, ištirti, ar alternatyvus valstybių patraukimo atsakomybėn būdas - tinkamo rūpestingumo („due diligence“) konceptas yra taikomas kaip privaloma elgesio norma kibernetiniame domene ir atsakyti į teisinį klausimą, ar tinkamo rūpestingumo koncepcija gali prisidėti prie priskyrimo problemos, susijusios su nevalstybinių veikėjų, kuriuos valstybės naudoja kaip marionetes, vykdomoms kibernetinėmis atakomis, išsprendimo? Šio darbo problematikos aktualumas yra pagrindžiamas tuo, jog pastaruoju metu teisės normos, kurios turėtų būti taikomos kibernetiniame domene, yra diskutuojamos įvairiuose tarptautiniuose forumuose (pvz., Vyriausybinių Ekspertų Grupėje), taip pat, konkrečiai tinkamo rūpestingumo klausimas pastaruoju metu susilaukė ir teisės mokslininkų dėmesio, tačiau galutinė šios grupės nuomonė ir mokslininkų pozicija ties tinkamo rūpestingumo klausimu išsiskiria. Nors ir egzistuoja valstybių praktikos (beje, gan ženklios), kuri teigia, kad konceptas yra taikomas kaip privaloma pareiga, visgi 2015 ir 2021 Vyriausybinių Ekspertų Grupės išvada buvo ta, jog principas yra savanoriškas ir neprivalomas, nors mokslininkai gan užtikrintai ir argumentuotai teigia, kad šis konceptas yra privalomas, tačiau pripažįsta, kad jo esmė vis dar nėra iki galo aiški.

Daugiausiai klausimų, visgi, kelia ne pats principo privalomumas, tačiau tai, kaip tiksliai ir kokia aprėptimi jis turėtų būti taikomas. Čia egzistuoja tam tikras konsensusas tarp valstybių ir teisės mokslininkų. Bent jau tuo aspektu, kad abi pusės pripažįsta, jog pačio principo taikymas yra neaiškus ir iki galo neapibrėžtas kibernetiniame domene. Tačiau šioje vietoje konsensusas ir baigiasi, čia turime ne tik nevienodą skirtingų valstybių poziciją, tačiau matome ir tam tikrus nesutarimus tarp teisės mokslininkų. Tam, kad būtų galima apibrėžti tinkamo rūpestingumo koncepto rėmus, tenka analizuoti tiek valstybių, tiek ir teismų praktiką, taip pat daug naudingų argumentų galima rasti Talino Manuale 2.0, kuris yra laikomas vienu autoritetingiausių mokslinių darbų, nagrinėjusiu normas, taikomas kibernetiniame domene. Kita vertus, patys Manualo autoriai nebuvo vieningos nuomonės dėl tam tikrų koncepto rėmų, todėl darbe yra analizuojami ir kitų autorių darbai, atliekamas lyginimas ir bandoma rasti principinius atsakymus.

Darbe buvo bandoma atsakyti į iškeltą hipotezę, kad tinkamo rūpestingumo koncepcija yra viena iš alternatyvų nebaudžiamumui panaikinti, šis principas taikytinas ir kibernetinėms operacijoms, o jo taikymas yra tikslingesnis būdas nustatyti valstybės atsakomybę dėl koncepto liberalumo.

Detaliai išanalizavus valstybių ir teismų praktiką, mokslininkų darbus buvo prieita prie iškelto teisinio klausimo atsakymo, kuris yra teigiamas - tinkamo rūpestingumo principas gali prisidėti prie priskyrimo problemos išsprendimo kibernetiniame domene, tačiau pats konceptas

ISSN 2029-4239 (online)
Teisės apžvalga
Law review
No. 2 (26), 2022, p. 4-30

vis dar turi būti vystomas ir aiškinamas tam, kad būtų galima jį naudoti efektyviau ir liktų mažiau neaiškumų pačioms valstybėms.

REIKŠMINIAI ŽODŽIAI

Kibernetinis tinkamo rūpestingumo principas, valstybių atsakomybė už kibernetines atakas, nevyriausybiniai veikėjai.