European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2022.01.63

SLCMC 2021
International conference «State and law in the context of modern challenges»

THE INTERNATIONAL LEGAL OBLIGATION OF DUE DILIGENCE IN CYBERSPACE

Nadezhda N. Lipkina (a)*, Dmitry V. Krasikov (b)
*Corresponding author

(a) Saratov State Law Academy, 1, Volskaya Str., Saratov, 410056, Russia, n_lipkina@list.ru

Abstract

The obligation of due diligence in international law corresponds to a generally recognized international legal duty of States to not let their territory to be used harmfully for other States. Recently, the attention towards this obligation in the theory and practice of international law has increased in the context of the discussion of application of existing rules of international law to cyberspace. In the light of recognizing the applicability of the general international principle of due diligence to the behaviour of States in this field, the questions arise of its effectiveness and sufficiency and of whether the development of a specific standard adapted to the peculiarities of cyber relations is required. The present paper deals with assessing the advantages and disadvantages of maintaining and using a general international legal standard for due diligence in cyberspace and the corresponding advantages and disadvantages of the prospect of elaborating a *lex specialis* standard. The main idea is that in the absence of a specific due diligence standard in cyberspace, there is no legal vacuum regarding the responsibility of a State in relation to an act that cannot be attributed to it, since there is a general international legal principle of due diligence. Besides, this principle has several advantages over potential special regulations that may appear in the future. In case of drafting such specific rules, it is necessary to proceed with caution and to take into account the shortcomings of special legal regulation.

2357-1330 © 2022 Published by European Publisher.

Keywords: Due diligence, cyberspace, Tallinn Manual 2.0

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Noncommercial 4.0 Unported License, permitting all non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.15405/epsbs.2022.01.63
Corresponding Author: Nadezhda N. Lipkina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

Currently, the scholarly and practical interest towards the international legal concept of due diligence is increasing greatly due to its significance within the discussion on regulation of States' conduct in cyberspace.

According to the International Court of Justice in the *Corfu Channel* case, "it is every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States". Despite the recognition and application of this obligation in authoritative case-law of the ICJ and other international bodies, doctrinal discussions are still ongoing about its nature, content, its acquisition of the character of a principle of international law, and even its existence as an obligation of general international law (Boon, 2014; McDonald, 2019).

Numerous studies comment on the due diligence obligation in particular branches of international law – international environmental law (Yotova, 2016), the law of armed conflict (Berkes, 2018), international human rights law (Monnheimer, 2021). Since there are special due diligence rules in certain areas, their relationship with the general due diligence standard is widely discussed (although there is also an opinion that international law does not contain a general principle of due diligence (McDonald, 2019)).

In the context of legal regulation of States' relations in cyberspace, due diligence can generally be understood as a States' obligation to not let their territory to be used for any cyber activities causing harm to other States.

In the light of the ongoing debate on the applicability of international law to cyberspace and its sufficiency to regulate cyber relations, the issue of States' duty to exercise due diligence within their territories and even abroad to prevent cyber harm becomes especially relevant primarily due to the problems of implementation of international responsibility in this area, caused by difficulties of attribution of private behavior to States (Jensen & Watts, 2017).

2. Problem Statement

The international team of experts working on the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (hereafter – Tallinn Manual 2.0) – one of the most authoritative studies on the application of international law to cyberspace – have included the principle of due diligence in its Rule 6 (Schmitt, 2017). The authors did not support the view that the general principle of due diligence and its application in the context of cyber operations did not achieve the *lex lata* status (the authors of this study assume that the whole set of Tallinn Manual 2.0 has got such status, although some researchers express doubts in this regard (Boer, 2019; Efrony & Shany, 2018)).

The issues of sufficiency of existing international law rules to regulate cyber relations and of the need to adopt any special rules are the subject of discussion among States. Some of them declare the need for a special binding instrument for cyberspace, while others consider it necessary to focus on determining how existing international law is applied in this area (as evidenced by the 2020 discussion within the UN Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security). One way or another, when considering a new treaty or when exchanging views on the modalities of application of the existing rule on due

https://doi.org/10.15405/epsbs.2022.01.63
Corresponding Author: Nadezhda N. Lipkina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

diligence, the question arises whether to maintain the relevant general standard or whether it is reasonable to move towards a standard specifically adapted to cyberspace.

3. Research Questions

The present study focuses on assessing the advantages and disadvantages of using a general international legal standard for due diligence in cyberspace, compared with the corresponding pros and cons of the idea of developing a *lex specialis* standard for the area. Accordingly, the main research questions are the following:

1. What are the advantages of maintaining and using a general due diligence standard for cyberspace (and the corresponding drawbacks of adopting a new standard)?
2. What are the advantages of adopting a specific international due diligence standard for cyberspace (and the corresponding problems of maintaining the general standard)?

4. Purpose of the Study

The purpose of this study is to assess the need to adapt the general due diligence standard for the field of public relations in cyberspace in terms of its suitability and effectiveness for enhancing international security, as well as for increasing the involvement of States in countering malicious behavior of third parties, on the one hand, and ensuring justice by refraining from imposing disproportionate burdens on States, on the other.

5. Research Methods

The research is based on the methods of analysis and synthesis, formal legal and comparative legal methods. The material studied covers academic comments on the problems of implementation of the due diligence principle in various areas of international law, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, as well as international case-law related to the issue of the States' duty of due diligence.

6. Findings

The obligation of due diligence is recognized by various treaty and customary international law regimes and is a principle of public international law applicable to all States' obligations of conduct (Kulesza, 2016). The advantages and disadvantages of securing this obligation for cyberspace it its general form, as well as those of elaborating a new rule specifically designed for cyber relations are determined by the vague and flexible character of the general due diligence standard and by the peculiarities of cyber conduct.

https://doi.org/10.15405/epsbs.2022.01.63
Corresponding Author: Nadezhda N. Lipkina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

6.1. The advantages of maintaining and using the general due diligence standard to regulate cyber conduct

The general international legal principle of due diligence is applicable to cyber relations and despite the fact that cyber relations differ notably from those in other areas, maintaining and using the general due diligence standard in cyberspace has certain advantages.

The general due diligence standard retains a significant degree of autonomy and flexibility for States in fulfilling their international obligations (French & Stephens, 2016). That is, it refers to the standard of conduct applicable to the primary norms of international law and does not contain a specific set of actions necessary to satisfy the requirements of the duty. It has so close relationship with primary rules that it is impossible to define it precisely (Boon, 2014), and commentators mainly propose certain core factors related to its content. One proposed set of factors includes reasonableness, the degree of State's control over relevant territory and over non-State actors, the degree of risk of harm, State's knowledge of such risk or of respective activity, and State's reaction (whether it acted in bad faith or did not act at all) (French & Stephens, 2016). The test used in the Tallinn Manual 2.0 Rule 7 contains the criteria of feasibility of the relevant measures to be taken (Schmitt, 2017).

Operation of the general standard does not exclude its specification when applied in certain particular areas of international law. The test proposed by the Tallinn Manual 2.0 (supplemented with the experts' comments) is presented as an application of the general standard but allows the authors to draw specific conclusions about its implementation in cyberspace, including particular criteria and limits (for example, the authors insist that States have no obligation to monitor cyber activities) (Schmitt, 2017).

Adopting a specified due diligence standard would lead to the loss of such advantages as flexibility and autonomy for States and this process would also reduce the likelihood of reaching a consensus on the content of such a standard among States. Maintaining the duty of due diligence as a general principle allows one to avoid difficulties of negotiating on any precise rules (French & Stephens, 2016). Moreover, it is not only difficult to receive States' consent to adopt a new rule, it is not easy to draft a new reliable and effective standard. How to define its content exhaustively? What degree of specificity should it have? While answering these questions it should also be taken into account that excessive concretization leads to more conflict with other rules and can make the rule obsolete over time.

Additionally, co-existence of the general standard with respective rules of special international legal regimes (such as international human rights law, environmental law or counter-terrorism law) does not raise conflicts, while different standards within the regimes need to be positively reconciled. If a specific due diligence standard for cyberspace is adopted, how will it relate to the respective approaches of international human rights law or of international counter-terrorism regulations? For example, the simultaneous effect of multiply special standards may raise problems in the context of "multispeed" evolutive development of norms in different areas.

https://doi.org/10.15405/epsbs.2022.01.63
Corresponding Author: Nadezhda N. Lipkina
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

6.2. The advantages of adopting a *lex specialis* due diligence standard for cyberspace regulation

One of the main disadvantages of the general international law principle of due diligence is that its overly general nature makes it vulnerable to criticism: it can be argued that it does not allow to reliably understand what exactly is required by this rule. Accordingly, a State cannot be always and absolutely sure that it duly complies with this obligation. The content of the rule and even its binding character is subject to debate (Moynihan, 2019). On the one hand, some commentators suggest that the due diligence principle contains sub-duties and sub-obligations such as an obligation to take the necessary legislative measures, an obligation to investigate the circumstances of the wrongdoings, an obligation to prosecute the perpetrators (Jensen, 2014; Sklerov, 2009). Also, it is argued that the obligation to prevent is a subsidiary to due diligence (White, 2012). On the other hand, for example, the authors of the Tallinn Manual 2.0 noted that an obligation "to take material preventive steps" cannot be inferred from the general principle under consideration (Schmitt, 2017).

Specifying the due diligence standard in relation to cyberspace will increase the level of legal certainty in the field and will allow one to strengthen or weaken the requirements of the general rule (for instance, the law of diplomatic missions enshrines a relatively high standard of the States' duty to protect missions' premises (French & Stephens, 2016)). Potentially, when drafting a new standard, States can take into account the shortcomings of the current practice of applying the general principle and the peculiarities of the relationship between the due diligence obligation and the rules of the law of international responsibility concerning attribution of conduct.

Another argument in favor of a special due diligence standard is that it can distinguish between "cyber-savvy" and "cyber-naïve" states (depending on their cyber assets and capabilities), making certain concessions for the latter concerning the standard of conduct or result.

Besides, adopting a new due diligence standard for cyberspace (if properly and cautiously drafted) will allow one to build it into the current system of specific due diligence standards in other areas, to determine how they correlate and balance, to arrange the modalities of its implementation, to fix relevant exceptions (if any).

7. Conclusion

There is no doubt that the general international legal principle of due diligence is applicable to international relations in cyberspace. This conclusion is based on the generally recognized consensus regarding the applicability of the existing rules of international law to this area in the absence of relevant *lex specialis*.

Any special due diligence standard in cyberspace has hardly been formed yet. At the same time, the controversial nature of general issues about the need for international lawmaking in the field of cyber law in general, as well as about the methods of international lawmaking relevant to the creation of such standards, also has an inhibitory effect on creating a new respective rule.

Taking into account the advantages and disadvantages of maintaining the general standard and elaborating a new standard, it can be concluded that the proper approach lies somewhere in the middle.

Specification of the due diligence standard is needed in cases where there is a vital necessity to raise or to lower the general standard in the light of particular peculiarities of cyber relations and where it is necessary to fill apparent gaps in the general standard. On the other hand, over-specification of regulation should be avoided. A special standard *per se* does not improve efficiency, and in case of drafting any relevant specific rules, it is necessary to proceed with caution and to take into account the shortcomings of special legal regulation.

Acknowledgments

The present paper is a part of the project "Theory-to-practice model of endorsement of territorial sovereignty and delimitation of States' jurisdictions in cyberspace" supported by the Russian Foundation for Basic Research (RFBR Grant No. 20-011-00806).

References

Berkes, A. (2018). The Standard of 'Due Diligence' as a Result of Interchange between the Law of Armed Conflict and General International Law. *Journal of Conflict and Security Law, 23*(3), 433–460. https://doi.org/10.1093/jcsl/kry022

Boer, L. (2019). *Lex Lata* comes with a Date; or, What Follows from Referring to the "Tallinn Rules". *American Journal of International Law Unbound, 113*, 76–80. https://doi.org/10.1017/aju.2019.11

Boon, K. E. (2014). Are Control Tests Fit for the Future? The Slippage Problem in Attribution Doctrines. *Melbourne Journal of International Law, 15*(2), 330–377.

Efrony, D., & Shany, Y. (2018). A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. *American Journal of International Law, 112*(4), 583–657. https://doi.org/10.1017/ajil.2018.86

French, D., & Stephens, T. (2016). *ILA Study Group on Due Diligence in International Law (Second Report, International Law Association, July 2016).* https://ila.vettoreweb.com/Storage/Download.aspx?DbStorageId=1427&StorageFileGuid=ed229726-4796-47f2-b891-8cafa221685f

Jensen, E. T. (2014). Cyber Sovereignty: The Way Ahead. *Texas International Law Journal, 50*(2), 275–304.

Jensen, E. T., & Watts, S. (2017). A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer? *Texas Law Review, 95*, 1555–1577.

Kulesza, J. (2016). *Due Diligence in International Law.* Brill|Nijhoff. https://doi.org/10.1163/9789004325197

McDonald, N. (2019). The Role of Due Diligence in International Law. *International and Comparative Law Quarterly, 68*(4), 1041–1054. https://doi.org/10.1017/S0020589319000344

Monnheimer, M. (2021). *Due Diligence Obligations in International Human Rights Law*. Cambridge University Press. https://doi.org/10.1017/9781108894784

Moynihan, H. (2019). *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention.* The Royal Institute of International Affairs Chatham House.

Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781316822524

Sklerov, M. J. (2009). Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defences against States Who Neglect Their Duty to Prevent. *Military Law Review, 201*, 1–85.

White, N. D. (2012). Due Diligence Obligations of Conduct: Developing a Responsibility Regime for PMSCs. *Criminal Justice Ethics, 31*(3), 233–261. https://doi.org/10.1080/0731129x.2012.738975

Yotova, R. (2016). The Principles of Due Diligence and Prevention in International Environmental Law. *The Cambridge Law Journal, 75*(3), 445–448. https://doi.org/10.1017/s0008197316000672