European Proceedings of
Social and Behavioural Sciences
EpSBS

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

DOI: 10.15405/epsbs.2022.01.58

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

INTERNATIONAL RESPONSIBILITY IN CYBERSPACE: THE PROBLEMS OF ATTRIBUTION OF CONDUCT

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

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

Abstract

Investigation and qualification of cyber incidents of a cross-border nature are complicated by difficulties to identify the device from which the attack was carried out, to establish the true place of the malicious activity, to identify specific responsible persons, and to assess their relationship with a State that may be involved in the cyberattack. This makes it problematic to attribute the harmful activity to such State for the purposes of international responsibility. Within the scholarly discussions, various options for overcoming these problems of attribution are proposed, among which two approaches are the most noticeable. One such option is to mitigate the attribution dilemma by laying stress on States' duty of due diligence. Another route is to elaborate a *lex specialis* "lightweight" test for attribution of non-State actors' conduct to States, namely the test of "control and capabilities". This paper contains the authors' comment on the ways proposed by scholars to overcome the problems of implementation of the international legal responsibility of States in cyberspace, generated by the difficulties of attribution of conduct. The authors advocate the view that the international obligation of due diligence and a more flexible control test for attribution may actually serve as a means of solving the attribution problems in cyberspace, but they are not without drawbacks, related to the nature of the proposed rules, their content, as well as their political effect, and these should be taken into account in the further discussion of ways out of the current situation of lack of effective tools.

Keywords: Attribution of conduct, due diligence, effective control test, international responsibility

https://doi.org/10.15405/epsbs.2022.01.58
Corresponding Author: Dmitry V. Krasikov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

The applicability of existing international law to the behavior of states in cyberspace has now become a somewhat contradictory concept. On the one hand, a number of international documents (claiming the status of reflecting the generally recognized position of the international community) insist on applicability of fundamental principles of international law and its existing rules to cyber conduct. On the other hand, the discussion of these issues in other formats demonstrates differences in the respective positions of states. While the results of the work of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (hereafter – the GGE) presume the existing consensus on the applicability of international legal rules to cyber relations. They also presume the current dialogue within the UN Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (hereafter – the OEWG) shows that some states (including Russia, China, Venezuela) advocate the existence of legal vacuum with regard to the behavior of states in cyberspace (at least in certain areas). And they urge the international community to negotiate an appropriate international treaty for the field (Boothby, 2019; Stadnik, 2017).

The problem is complicated by the fact that often the subject of discussion is the applicability to cyber relations of a set of principles of international law – rather broad and vague regulators (some of which are even discussed with regard to whether they enshrine any specific rules (Corn & Taylor, 2017)), or the question is raised about the abstract applicability of a certain entire set of international legal norms to cyberspace, which obviously can only lead to the expression of overly general positions without any regard to particular specific circumstances of potential cyber incidents. As a result, the statements about the applicability of international legal rules to cyberspace can hardly be perceived as covering all rules *without any exception*, while those on legal vacuum – as advocating an *absolute* vacuum.

In such circumstances, the discussion of the applicability of specific rules or sets of rules to specific relations in cyberspace becomes most relevant within the debate (Moynihan, 2019). The law of international responsibility serves as a vivid illustration of both the divergence of States' opinions regarding the regulation of international cyber relations, and the lack of clarity regarding the modalities of application of the existing norms in this field. Although some authoritative studies proceed from the point that customary international law of State responsibility undeniably extends to cyber activities and focus on how it is applied (Schmitt, 2017), in practice there are objections even to its applicability *par se* (e.g. China's position within the OEWG). Such discrepancies and the lack of clarity are explained by the problems related to the unique nature of cyberspace. And one of the most significant problems concerns attribution of cyber conduct in the context of international responsibility of States. The cross-border nature of cyber incidents and the corresponding difficulties in investigating the factual circumstances of cyberattacks include identification of devices that served as means of committing cross-border malicious acts, the identity of the attacker, the place of the act, etc. (Jensen & Watts, 2017). They hinder the implementation of legal responsibility in international relations and urge researchers and practitioners to seek for ways of overcoming these obstacles.

https://doi.org/10.15405/epsbs.2022.01.58
Corresponding Author: Dmitry V. Krasikov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

2. Problem Statement

Investigation and qualification of cyber incidents of a cross-border nature are complicated by the fact that it may be difficult for an injured state to identify the device from which the attack was carried out, to establish the true place of the malicious activity, to identify specific responsible persons, and even more so, to assess their relationship with a State that may be involved in the cyberattack. At the same time, in the absence of relevant information, it is impossible to properly establish the existence of grounds for bringing a potentially implicated State to international responsibility: attribution of conduct (along with a breach of a State's international obligation) is an necessary element of an internationally wrongful act (as follows from Article 2 of the International Law Commission Articles on Responsibility of States for Internationally Wrongful Acts (hereafter – ILC Articles)), and qualifying a cyberattack as such wrongful act requires establishing a proper link between the conduct of persons who directly committed the act, and the State.

Within the scholarly discussions, various options for overcoming these problems of attribution are proposed, among which two approaches are the most noticeable. One such option is to mitigate the attribution dilemma by laying stress on States' duty of due diligence (Jensen & Watts, 2017). An alternative (or an additional) route is to elaborate a *lex specialis* "lightweight" test for attribution of non-State actors' conduct to States, namely the test of "control and capabilities" (Stockburger, 2017).

On the one hand, in the context of the ongoing discussion about the sufficiency and suitability of the existing international legal rules for regulating international relations in cyberspace, the ideas expressed in scholarship about the need to adapt or even to modify general international law rules can be seen as overly far-reaching initiatives. On the other hand, the problems of cyber relations regulation undoubtedly require a solution, and regardless of the prospects and mechanisms for validating the above approaches, as well as of their justifiability, an assessment of their suitability for overcoming the problems of attribution seems necessary.

3. Research Questions

The main research questions concern the extent to which an emphasis on the duty of due diligence and the test of "control and capabilities", as proposed in scholarship, can serve as effective means of overcoming the difficulties of attribution of cyber conduct.

1. What are the potential problems of relying on the duty of due diligence as a means to overcome the difficulties of attribution of conduct in cyberspace?
2. What are the potential problems of using the test of "control and capabilities" as a means to overcome the difficulties of attribution of conduct in cyberspace?

4. Purpose of the Study

The purpose of this study is to assess the ways proposed by researchers to overcome the obstacles in the implementation of international legal responsibility for States' conduct in cyberspace, caused by the attribution problems.

https://doi.org/10.15405/epsbs.2022.01.58
Corresponding Author: Dmitry V. Krasikov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

5. Research Methods

The research is based on methods of analysis and synthesis, formal legal and comparative legal methods. The material studied includes academic works on the issue of legal regulation of cyberspace, the GGE Reports of, the States' comments on the 2020 Initial "Pre-draft" of the OEWG Report, the Tallinn Manual 2.0, ILC Articles with commentaries, as well as relevant ICJ case-law.

6. Findings

Both approaches – making use of the States' duty of due diligence and elaborating a new test for attribution – are widely discussed as means of overcoming the cyber attribution problems, and both, being not completely new for international law, represent either sort of adaptation (as is the case of due diligence) or modification (as is the *lex specialis* proposal) of existing international legal rules in their application to new cyber relations.

The obligation of due diligence forms part of general international law and is considered to be applicable in cyber context, as follows, in particular, from the position of the group of authors of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (hereafter – Tallinn Manual 2.0) (Schmitt, 2017). And in its turn, the idea of using a specific attribution standard deviates from the conventional test of effective control, used, in particular, by the International Court of Justice (ICJ) in the case of *Military and Paramilitary Activities in and against Nicaragua* and in the *Case concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide*.

The two subsections below comment on the potential problems related to both approaches from the perspective of their serving as means to overcome the cyber attribution problems.

6.1. The obligation of due diligence

In circumstances where rigorous control tests are ineffective, one of the preferred regulatory strategies is to place an emphasis on the responsibility to prevent negative consequences of conduct (Boon, 2014), and one way to alleviate the cyberspace attribution dilemma is to make use of the States' duty of due diligence (Jensen & Watts, 2017). According to Rule 6 of the Tallinn Manual 2.0, "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" (Schmitt, 2017, p. 30).

The idea of using this obligation to overcome the problems of attribution of cyber conduct is to invoke the responsibility of a State notwithstanding lack of evidence necessary to consider the malicious conduct as an act of this State. To what extent can this duty be an effective means of overcoming the complexities of attribution?

First, due diligence forms part of primary general international law rules, and the qualification of non-compliance with this obligation may also present certain evidentiary difficulties (at least, as concerns the "under governmental control" part of the rule). Second, there is no clarity about the content of this obligation, and namely about the relevant "sub-duties". For example, while due diligence as such is often

https://doi.org/10.15405/epsbs.2022.01.58
Corresponding Author: Dmitry V. Krasikov
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

associated with prevention, it is argued that it does not imply a general duty of prevention. Also, in the light of vagueness of the Tallinn Manual 2.0 "serious adverse consequences" criterion, it is not definitely clear what is the threshold for the harm necessary to find a violation. Third, the duty to take only feasible and reasonably available measures cannot cover the entire spectrum of possible circumstances of cyberattacks. Moreover, due diligence can only serve as a partial alternative to responsibility of a State for the cyberattack itself: basically, it has no relevant effect in a situation where a State has violated this obligation by not preventing a third State from using its cyber infrastructure for harmful purposes. In such cases, bringing to justice a State, whose cyber infrastructure is used by a third State for a malicious cyberattack, essentially allows the true violator to escape responsibility. Fourth, a significant emphasis on due diligence creates certain political risks: as argued by Jensen and Watts (2017), it can potentially increase the likelihood of destabilizing effects for international relations since it facilitates States' recourse to countermeasures.

Thus, while the duty of due diligence may have some effect on overcoming the cyberspace attribution problems, it cannot be seen as a full-fledged remedy.

6.2. The test of "control and capabilities"

According to the International Law Commission's commentary on art. 8 of the 2001 Draft articles on Responsibility of States for Internationally Wrongful Acts, a conduct "carried out under the direction or control of a State <…> will be attributable to the State only if it directed or controlled the specific operation and the conduct complained of was an integral part of that operation". As evidenced by the ICJ case-law mentioned above, the effective control test is one of the tools traditionally used for attribution of conduct of non-State actors to States and covers the "direction" and "control" clauses contained in art. 8 of the ILC Articles (Schmitt, 2017).

However, on the one hand, it can be problematic to establish such level of control as regards cyber conduct due to cross-border investigation obstacles and specificity of cyber conduct. On the other hand, the standard of attribution cannot be extremely low: as it was noted by the GGE in its 2015 Report, "the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State".

One way to deal with this problem is to elaborate a new *lex specialis* rule, reflecting a more flexible test for attribution of conduct in cyber realm. One such approach is proposed by Stockburger (2017), who advocates the test of "control and capabilities" as a tool for attribution of cyber conduct. The test is based on assessment of a number of factors, including *inter alia* the relationship between the State and the relevant non-State actor, any State's influence over the actor, the methods used by the relevant non-State actor, the State's and non-State actor's motivations, their technical capabilities and geographic factor (Stockburger, 2017).

Such approach can indeed help to overcome the attribution dilemma, but it has certain drawbacks. The proposed set of factors includes those related to the very factual issues which complicate using the test of effective control from the perspective of obtaining evidence. Thus, similar technical problems (concerning identity of users and their relationship with a State, location of infrastructure, distorted data, etc.) may arise. Also, the content of the criteria and the relevant standard of proof are not quite clear. As a

result, the test is more suitable for political not legal attribution. Besides, as with the case of due diligence, using more flexible test may create political risks by simplification the process of States' recourse to countermeasures.

7. Conclusion

Discussion of the problems related to implementation of States' responsibility in cyberspace and the search for relevant solutions is an important task of contemporary research and practice in the field of international law. At the same time, the proposed approaches require an assessment of their suitability for solving the corresponding problems.

The international obligation of due diligence and a more flexible control test for attribution may actually serve as a means of solving the attribution problems in cyberspace, but they are not without drawbacks, related to the nature of the proposed rules, their content, as well as their political effect, and these should be taken into account in the further discussion of ways out of the current situation of lack of effective tools. Further studies of the problems under consideration can be focused on revealing the content of the proposed rules, including their application to specific circumstances.

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

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.

Boothby, W. H. (2019). *New Technologies and the Law in War and Peace*. Cambridge University Press. https://doi.org/10.1017/9781108609388

Corn, G. P., & Taylor, R. (2017). Sovereignty in the age of cyber. *American Journal of International Law Unbound, 111*, 207–212. https://doi.org/10.1017/aju.2017.57

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

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

Stadnik, I. (2017). What is an International Cybersecurity Regime and how we can Achieve it? *Masaryk University Journal of Law and Technology, 11*(1), 129–154. https://doi.org/10.5817/MUJLT2017-1-7

Stockburger, P. Z. (2017). Control and capabilities test: Toward a new lex specialis governing state responsibility for third party cyber incidents. In *2017 9th International Conference on Cyber Conflict (CyCon)* (pp. 1–14). Curran Associates, Inc. https://doi.org/10.23919/cycon.2017.8240334