Legal Issues in the Digital Age. 2024. Vol. 5. No. 3.
Вопросы права в цифровую эпоху. 2024. Том 5. № 3.

International Law And Cybersecurity

Research article
УДК: 341
JEL: K33
DOI:10.17323/2713-2749.2024.3.103.128

Collective Countermeasures in Response to Cyber Operations under International Law

Ekaterina Aleksandrovna Martynova
Center for Technology and Society, Fundação Getulio Vargas (FGV) Law School, 190 Praia de Botafogo, Rio de Janeiro, CEP: 22250-900, Brazil,
eamartynova@hse.ru, ORCID id: 0000-0002-8995-4462

Abstract

The paper examines the application of collective countermeasures — i.e., measures taken by non-injured states — as a means of cooperative non-institutionalized response to malicious cyber-enabled activities undertaken or controlled by a state. Particularly, the paper investigates: the right of the state not injured by a cyber operation to take countermeasures against the perpetrating state under current international law; and state positions towards collective countermeasures and possible grounds for the development of a more supportive attitude within states to this form of collective reaction. General research and special legal methods, as well as game theory, are employed to test the hypothesis the concept of collective countermeasures has been gaining nascent and fragmented support by states in terms of its applicability in the context of cyber operations. The author concludes this emerging trend reflects the general tendency of states to join forces to halt malicious activities in cyberspace and impose political and economic costs upon the perpetrators. This allows one to assume that collective countermeasures in response to cyber operations might become an expectable means of reaction by 'like-minded' states. Their legitimation might, therefore, be determined not only (or not so much) by the development of international law due to the practical difficulty in harmonizing positions among states on this issue at the current stage, but rather as a part of the general political trend of uniting the efforts of states to bring wrongdoers in cyberspace to responsibility.

Keywords

cyberspace; cyber operations; state responsibility; countermeasures; Tallinn Manual 2.0; game theory.

For citation: Martynova E.A. (2024) Collective Countermeasures in Response to Cyber Operations Under International Law. *Legal Issues in the Digital Age,* vol. 5, no. 3, pp. 103–128. DOI:10.17323/2713-2749.2024.3.103.128

Introduction

The article examines whether a state, or a group of states, not injured by malicious cyber activities can employ countermeasures in assistance to the victim-state or independently of the latter. The term 'collective countermeasures' in the title of the paper, as well as the alternative term 'third-party countermeasures', are not defined in any legal source, including the most authoritative document on states responsibility — Articles on Responsibility of States for Internationally Wrongful Acts ('ARSIWA').[1] As will be described, the application of countermeasures by a non-injured state has been discussed by the UN International Law Commission (ILC) and the Sixth Committee of the UN General Assembly within the development of ARSIWA, as well as in legal scholarship, and turns out to be a truly divisive issue. In certain cases the distinction is made between 'third-party countermeasures' as measures taken by a non-injured state in the interest of the injured state, sometimes on behalf of or at the request of the latter, and 'collective countermeasures' as a means of congregate reaction to enforce a communitarian norm [Delerue F., 2020: 454].

The concept of third-party countermeasures under general (not cyber-specific) international law was examined in detail by Martin Dawidowicz in his seminal *Third-Party Countermeasures in International Law* [Dawidowicz M., 2017]. The academic discussion of collective responses to hostile cyber-enabled actions has intensified against the backdrop of increasing 'naming and shaming' of particular states in the systematic commission of wrongdoings in cyberspace [Finnemore M., Hollis D.B., 2020]. The body of scholarship on countermeasures presents a relative consensus that international law does not entitle a state, other than the victim-state,

[1] UNGA Res. 56/83. Articles on Responsibility of States for Internationally Wrongful Acts. 12 December 2001. UN Doc. A/RES/56/83.

to take countermeasures in response to a cyber operation [Tsagourias N., 2015]; [Henriksen A., 2015]; [Corn G., Jensen E.T., 2018]. At the same time, publications by European and American authors in recent years have increasingly expressed cautious support for the possibility of using collective countermeasures in cyberspace. In particular, there are arguments that international law has been evolving since ARSIWA to permit collective countermeasures in the cases when collective obligations are violated [Roguski P., 2020: 36]; that limited acceptability of collective countermeasures is justified by political reasons, such as the technological impossibility for some states to respond to a cyber-attack without the help of more cyber advanced allies [Haataja S., 2020: 49]; and — more generally — that international law does not contain a clear prohibition on collective countermeasures, and the overall development of international law towards a collectivist approach confirms rather than denies the legitimacy of collective countermeasures [Schmitt M.N., Watts S., 2021: 182, 200].

The Russian doctrine considers the concept of collective countermeasures, or countermeasures in the collective interest, both in the general theory of international responsibility [Lukashuk I.I., 2004: 355]; [Lipkina N.N., 2013: 49–50]; [Keshner M.V., 2017: 130–132] and, in particular, in the context of the legitimacy of collective coercive measures applied by the European Union, and other (often informal) associations of states, against the Russian Federation [Kozheurov Ya. S., 2015: 182]. Russian specialists tend to question the validity of such measures from the standpoint of the current development of international law [Kononova K. O., 2010: 16]; [Keshner M.V., 2015: 37, 47]. At the same time, the issues of the legality and practice of collective countermeasures as a response to hostile actions in cyberspace remains significantly understudied in the Russian doctrine. It appears that the specifics of cyberspace, cyber operations and responses to them, as well as the positions formed in official statements of states, predetermine the importance of reconsidering the legality of collective countermeasures specifically in relation to cyber operations. In this paper the terminological distinction between 'collective countermeasures' and 'third-party countermeasures' is provided when it is relevant to the issue under discussion; otherwise, the term 'collective countermeasures' is used as a more general term due to its prevalence in the literature devoted to state responsibility.

The paper aims to contribute to the current discussion on the admissibility of collective countermeasures in the cyber context in two ways. First, the most recent state practice and *opinio juris* have been analyzed including

the Official compendium of voluntary national contributions by states on the subject of how international law applies to the use of information and communications technologies (hereinafter Compendium)[2] and recently adopted national strategies on cyber security (particularly, the US National Cyber Security Strategy of 2023), as well as multilateral declarations on this matter. Second, the tools of analysis used in this paper include general scientific and special legal methods, along with application of beyond-positivistic research approaches to international law. Among the general research methods, the method of analysis was used, including the study of positions of states on the application of international law in cyberspace. The method of synthesis was employed to generalize the approaches of states to the legality of the measures applied to respond to cyber threats. The study also involved the application of methods of formal logic. In particular, the method of induction was used to identify collective countermeasures as a separate group of potential ways to influence states that allegedly commit malicious acts in cyberspace. The foresight method was employed to outline possible trajectories for the future development of states' cyber response strategies, in particular in analysing possible consensus-building on the legality of collective countermeasures in the context of cyber operations. Apart from the 'expository' tradition in legal research, contemplating study of legal texts, this study was conducted in the tradition of a methodological approach designated in literature as 'International Law and Economics' [Danielsen D., 2016: 453–488]. Namely, it employed game theory analysis to assess the possibility of a collective response to cyber operations by means of countermeasures, taking into account not only black-letter law, but also current political processes and incentives for states to act in a particular way.

The paper presented is structured as follows. The next section provides a brief overview of the concept of countermeasures in international law and positions of states on their applicability in cyberspace. Section Two describes the drafting history of ARSIWA with respect to the application of countermeasures by a state other than the state injured by an internationally wrongful act, which can be applied to understanding of why states are in

[2] 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 Behavior in Cyberspace in the Context of International Security, 13 July 2021. UN Doc. A/76/136. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/189/48/PDF/N2118948.pdf?OpenElement (accessed: 05.07.2024)

most cases indecisive in supporting collective countermeasures in the cyber context. Section Two also provides a beyond-positivistic analysis and suggests an assessment based on game theory to enrich the discussion on the admissibility of collective countermeasures based on political rather than purely legal grounds. Section Three is a comclusion.

1. Countermeasures and State Responsibility in Cyberspace

1.1. Notion of 'countermeasures' and its applicability in the cyber context

When a state is directly injured by another state's violation of obligations owed by the latter state to the former, international law allows to state to take countermeasures. The fact that there was a prior violation precludes the countermeasures from being themselves wrongful,[3] as countermeasures are understood as 'measures that would otherwise be contrary to the international obligations of an injured state *vis-à-vis* the responsible state, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation.'[4]

The substance of countermeasures is temporary non-performance by the state applying countermeasures of its international obligation (or several obligations simultaneously[5]) towards the responsible state.[6] Their purpose is to induce a wrongdoing state to comply with obligations of cessation and reparation towards the state taking the countermeasures. Accordingly, countermeasures may not have a coercive character;[7] they should be instrumental, but neither punitive[8] nor forcible.[9] Countermeasures should be

[3] Gabčikovo-Nagymaros Project (Hungary v. Slovakia), Merits, Judgment of 25 September 1997. ICJ Rep. 7, at 55 para 83: countermeasures might justify otherwise unlawful conduct 'taken in response to a previous international wrongful act of another state and ... directed against that state'.

[4] International Law Commission. Articles on the Responsibility of States for Internationally Wrongful Acts, with Commentaries (2001). UN Doc. A/56/10 (ARSIWA w. Commentaries). Part Three. Chapter II, para 1.

[5] ARSIWA w. Commentaries, commentary (6) to Art. 49.

[6] Ibid. Art. 49, para 2.

[7] ARSIWA w. Commentaries, commentary (3) to Art. 18.

[8] Ibid. Commentary (1) to art 49.

[9] ARSIWA. Art 50, para 1(a).

temporal ones[10] and reversible as far as possible.[11] They cannot coerce the wrongdoing state to violate obligations to third states[12] or involve any departure from certain norms of international law, including *jus cogens* norms.[13] Neither can they affect any dispute settlement procedure that is in force between the two states,[14] nor impair diplomatic or consular inviolability.[15]

As is well known, states conceptually affirm application of international law, and in particular the Charter of the UN, in the cyber context.[16] The Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security ('the GGE') has specifically addressed in several reports international obligations of states regarding internationally wrongful acts using information and communication technologies ('the ICTs').[17] The UN Open-Ended Working Group ('the OEWG') concluded in the 2021 Final Substantive Report on the need for further development of rules, norms and principles of responsible behavior of states in cyberspace.[18] However, none of the final reports of GGE or OEWG published to date contains their conclusions or proposals on the applicability of countermeasures in response to malicious activities in cyberspace.

Another widely cited source on the application of the norms of international law in the cyber context — the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations [Schmitt M. N., 2017] (hereinafter the Tallinn Manual 2.0) representing views of the international group of experts not including specialists from Russia — on the contrary, offers

[10] Ibid. Art. 49, para 2: 'for the time being'.

[11] Ibid. Art. 49, paras 2 and 3, and Art 53; ICJ, Gabcíkovo-Nagymaros Project, at 56–57, para 87.

[12] ARSIWA w. Commentaries, commentary (3) to Art. 18.

[13] ARSIWA Art. 50, para 1; Application of the Convention on the Prevention and Punishment of the Crime of Genocide, Counter-Claims, Order of 17 December 1997, ICJ. Reports 1997, at 258, para 35: 'in no case could one breach of the Convention serve as an excuse for another'.

[14] Ibid. Art. 50, para 2(a).

[15] Ibid.

[16] The General Assembly welcomed this affirmation of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) on numerous occasions: see UNGA Res. A/70/455. 23 December 2015.

[17] GGE Report 2013. UN Doc. A/68/98, para 23; GGE Report 2015. UN Doc. A/70/174, para 13; and GGE Report 2021. UN Doc. A/76/135, para 25.

[18] OEWG. Final Substantive Report 2021. UN Doc A/75/816, paras 8, 24.

comprehensive rules and commentary on countermeasures. The group of international experts who authored the Tallinn Manual 2.0 starts with a general statement about the right of a state injured by a cyber operation to employ countermeasures, 'whether cyber in nature or not', if the operation constitutes a breach of an international legal obligation owed by the wrongdoing state.[19] The Tallinn Manual 2.0 then clarifies the requirements for the countermeasures to be considered lawful, including limitations of the purpose and targets of countermeasures, their compliance with peremptory norms of international law, and the mode of their execution.[20]

Since recently (and particularly after the publication of the Tallinn Manual 2.0), several states began to indicate their position on the applicability of countermeasures as a means of response to malicious use of ICTs. Thus, Australia has specified, in 2017, that a state injured by malicious cyber activity attributable to another state may apply countermeasures if they are non-forcible, proportionate and aimed at compelling the perpetrator state to cease the wrongful conduct;[21] in 2020 Australia has reaffirmed, in a comprehensive case study, its position on the legality of countermeasures in response to hostile conduct using ICTs if the measures applied meet the requirements of proportionality, reversibility, non-forcible character, compliance with fundamental human rights, humanitarian obligations and peremptory norms of international law.[22] Canada enumerates similar constraints for states to take countermeasures in response to cyber operations; herewith, the position of Canada is quite specific in respect of the attribution of the relevant malicious conduct to the responsible state: a state taking countermeasures is not obliged to provide detailed information equivalent to the level of evidence required in a judicial process to justify its cyber countermeasures; however, the state should have reasonable grounds to believe that the state that is alleged to have committed the internationally wrongful act was responsible for it.[23]

---

[19] Tallinn Manual 2.0. Rule 20.

[20] Ibid. Rules 21–23.

[21] Australia's International Cyber Engagement Strategy 2017. Available at: www.internationalcybertech.gov.au/about/2017-International-Cyber-Engagement-Strategy (accessed: 05.07.2024)

[22] Case studies on the application of international law in cyberspace, published February 2020. Available at: www.internationalcybertech.gov.au/sites/default/files/2020-12/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf, at 3 (accessed: 05.07.2024)

[23] Government of Canada. International Law applicable in cyberspace. Available at: www.international.gc.ca/world-monde/issues_development-enjeux_developpement/

France, in its submission to the OEWG in 2021, indicated it considers itself entitled to take cyber-related countermeasures 'designed to (i) protect its interests and ensure they are respected and (ii) induce the state responsible to comply with its obligations',[24] thus broadening the legitimate purpose of the application of countermeasures by indicating the goal of protection of interests without specifying their scope. Germany and Norway, likewise, have stated that malicious use of ICTs can be responded to by countermeasures; at the same time, they share a cautious approach to their application due to 'multifold and close interlinkage of cyber infrastructures not only across different states but also across different institutions and segments of society within states'[25] and the difficulties in the attribution of cyber operations to the responsible state.[26] Switzerland,[27] the UK[28] and the US[29] similarly maintain that a state injured by malicious cyber-enabled activities which constitute internationally wrongful acts may resort to countermeasures subject that general requirements contemplated by international law to this means of response are met. Overall, there is agreement among the named states that countermeasures may be both of cyber and non-cyber nature.

China stands out from the crowd claiming that the law of state responsibility 'has not yet gained international consensus', and '*there is no legal basis at all* for any discussion on its application in cyberspace'.[30] More generally, China questions the utility of enforcing rules on countermeasures enshrined in ARSIWA in the cyber context — instead, it advocates for the

---

peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a9, para 34-36 (accessed: 05.07.2024)

[24] International Law Applied to Operations in Cyberspace, Paper shared by France with the Open-ended working group established by resolution 75/240. Available at: https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf, at 4 (accessed: 05.07.2024)

[25] Position Paper on the Application of International Law in Cyberspace, submitted by Germany to OEWG. 2021. Available at: https://documents.unoda.org/wp-content/uploads/2021/12/Germany-Position-Paper-On-the-Application-of-International-Law-in-Cyberspace.pdf, at 13–14 (accessed: 05.07.2024)

[26] Compendium, 72–73.

[27] Ibid, 90–91.

[28] Ibid, 118.

[29] Ibid, 142.

[30] China's Contribution to the Initial Pre-Draft of OEWG Report. Available at: https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf, at 5 (emphasis added) (accessed: 06.07.2024)

application of general principles of international law reflected in the UN Charter. To date, this position appears to be a rare exception and is rather intended to emphasize the commitment of Chinese experts to the idea of the development of new international treaties to establish binding rules of state behaviour in cyberspace [Huang Z., Ying Y., 2021: 555–558].

Another BRICS country, Brazil, also takes a cautious stance on responding to cyber operations by countermeasures: 'Brazil considers that there needs to be further discussions on the legality of countermeasures as a response to internationally wrongful acts, including in the cyber context'.[31] This wariness is based on the premise that the ARSIWA provisions on countermeasures went beyond codification of customary norms and represent a progressive development of international law,[32] which at least calls into question the states' obligation to follow them, as well as concerns about the feasibility of meeting the procedural requirements of application countermeasures in the ICTs environment.

Unlike retorsions being 'unfriendly conduct which is not inconsistent with any international obligation of the state engaging in it',[33] acts (or omissions) that constitute countermeasures would normally be wrongful unless certain conditions are met.

Firstly, the existence of an internationally wrongful act towards the states applying countermeasures should be established.[34] This necessitates the attribution of the relevant conduct to the responsible state [Shany Y., Schmitt M. N., 2020]; [Lahmann H., 2020] and qualification of a cyber operation as a violation of a particular obligation which the responsible state owes to the injured state. The literature on the application of international law in cyberspace considers the possibility of qualifying cyber operations, inter alia, as violations of the principle to respect state sovereignty [Rusinova V., Assaf A., Moshnikov D., 2020]; [Coco A., Dias T., van Benthem T., 2022]; the principle of non-intervention [Watts S., 2015]; the prohibition of the use of force and/or qualification of the cyber incident as an armed attack [Roscini M., 2014].

[31] Compendium, 22.

[32] Max Planck Encyclopedia of International Law. Countermeasures (2015).

[33] ARSIWA w. Commentaries. Chapter II. Countermeasures, commentary (3).

[34] ICJ, Gabcíkovo-Nagymaros Project, at 55 para 83: 'In the first place it must be taken in response to a previous international wrongful act of another state and must be directed against that state'.

Secondly, the countermeasures applied must comply with the proportionality test, i.e. they should take into account the gravity of the internationally wrongful act and the rights in question.[35] The Tallinn Manual 2.0 offers a rather vague definition of 'injury', which is taken into account when assessing proportionality of countermeasures applied in response to malicious cyber-enabled activities: it 'is not to be understood to require damage. Instead, simple breach of an international legal obligation suffices to make proportionate countermeasures available to the injured state.'[36] It seems that such an approach contradicts the position of the ILC which points to proportionality as 'an essential limit'[37] of the intensity of countermeasures, which also serves as a protection for the injured state itself from being subjected to the rules of responsibility. The mandatory proportionality of countermeasures was confirmed by the majority of states that declared their position on the state responsibility for malicious activities in cyberspace (including, during the sessions of the OEWG): among them, Germany underlines that states should be especially cautious and prudent when determining whether the applicable constraining criteria for cyber countermeasures are met, and if such actions satisfy the standards for countermeasures, a state may — *a maiore ad minus* — engage in cyber reconnaissance measures to investigate options for countermeasures and evaluate the potential danger of side effects.[38]

Finally, countermeasures may be justified only if taken against the wrongdoing state and do not affect third parties.[39] This requirement is of particular importance in the context of cyber-enabled countermeasures because, as noted by Brazil, 'cyber operations can be designed to mask or spoof the perpetrator, which in turn increases the risks of miscalculated responses against innocent actors'.[40]

---

[35] ARSIWA. Art. 51; Case Concerning the Air Service Agreement of 27 March 1946 between the United States of America and France, Decision of 9 December 1978, UN Reports of international arbitral awards, Vol. XVIII, at 443-444 para 83.

[36] Tallinn Manual 2.0, commentary 2 to Rule 23.

[37] ARSIWA w. Commentaries, commentary (1) to Art. 51.

[38] Position Paper on the Application of International Law in Cyberspace, submitted by Germany to OEWG, 2021. Available at: https://documents.unoda.org/wp-content/uploads/2021/12/Germany-Position-Paper-On-the-Application-of-International-Law-in-Cyberspace.pdf, at 13–14 (accessed: 06.07.2024)

[39] ARSIWA. Art. 49, para 1 and 2.

[40] Compendium, 22.

2. Substantive and Procedural Requirements to Countermeasures: Is *Lex Specialis* Needed for Cyber Countermeasures?

Apart from the substantive restrictions described above, the use of countermeasures must meet certain procedural requirements. Article 52 of ARSIWA imposes two main procedural duties on a state intending to resort to countermeasures: to call upon the wrongdoing state to comply with its obligations[41] (obligation also known as '*sommation'*[42]*); and to notify the responsible state of its intention to apply countermeasures and offer negotiation. That said, in emergency circumstances, the injured state is permitted to forego the requirement of notification and offer negotiations and take urgent* countermeasures 'as are necessary to preserve its rights'.[43] Such relief, however, does not apply to the *sommation*.

The Tallinn Manual 2.0 provides a non-exhaustive list of examples where urgent cyber countermeasures can justify waiver of prior notification requirement: (i) when the injured state needs to take prompt action to protect its rights and prevent further harm;[44] and (ii) when prior notification of the intent to take a countermeasure will make it meaningless.[45] While the minority of experts, authors of the Tallinn Manual 2.0 came to the conclusion that customary international law (specifically, Article 52(1)(b) ARSIWA) requires the injured state to seek negotiations before taking countermeasures, the majority of them rejected this requirement and argued that an injured state may take countermeasures before seeking negotiations.[46]

An analysis of available states' positions on the applicability of the requirements set forth in Article 52 of ARSIWA to cyber-related countermeasures has revealed the following. First, a number of states which have expressed their position on applicability of the rules on countermeasures

[41] ARSIWA. Art 52(1)(a). Jurisprudence on sommation: Air Service Agreement, at 444, paras 85-87; Gabcíkovo-Nagymaros Project, at 56, para 84. See also: G. Arangio-Ruiz. Fourth Report on State Responsibility. 1992 YILC. Vol. II, 22, para 6ff.

[42] ARSIWA w. Commentaries, commentary (3) to Art. 52.

[43] Art. 52(2) of ARSIWA, ARSIWA w. Commentaries, commentary (5) to Art. 52: temporal relationship between the operation of subparagraphs (a) and (b) of paragraph 1 is not strict. Notifications could be made close to each other or even at the same time.

[44] Tallinn Manual 2.0, commentary 11 to Rule 21.

[45] Ibid. Commentary 12 to Rule 21.

[46] Ibid. Commentary 13 to Rule 21.

in response to cyber operations (including Australia, Denmark, Estonia, and Germany) omit addressing procedural requirements altogether. Out of this group of states, Canada indicates that the precise scope of certain procedural aspects of countermeasures, such as notification, 'needs to be further defined through state practice given the unique nature of cyberspace'[47] (leaving, however, open the question of whether requirements contemplated by ARSIWA are generally appropriate for the cyber domain).

Second, only two states, Italy and Norway, distinguish between the two requirements stipulated by Article 52(1) of ARSIWA: to call upon the responsible state to fulfill its obligations, and to notify it of the decision to take countermeasures and offer to negotiate. Herewith, Italy indicates that derogation from both requirements is possible in cases of emergency[48], which contradicts the idea of urgent countermeasures implied by the ILC. Norway seems to be the closest to the provisions of Article 52(2) of ARSIWA, indicating that urgent countermeasures can be taken without prior notification 'if providing such notification might reveal sensitive methods or capabilities or prevent the countermeasures from having the necessary effect', and not saying the same regarding the requirement to request the responsible state to fulfill its obligations.[49]

Finally, the rest of the states mention only one of the procedural requirements or indicate both but do not differentiate exceptions, in cases of an urgent countermeasure. For instance, France acknowledges the obligation of the victim-state to notify the responsible state of its intention to take countermeasures, which the obligation can be derogated from if the injured state needs to protect its rights (but doesn't mention the *sommation*).[50] Switzerland indicates that 'the responsible state can only impose countermeasures if it has first called for the violation(s) to cease and has announced what measures it is planning to take' and, at the same time, '[e]xceptions may be made for cyber operations requiring an immediate response in order for the injured state to enforce its rights and prevent further damage'[51]

[47] Government of Canada. International Law applicable in cyberspace (no. 33), para 36.

[48] Italian Position Paper on 'International Law and Cyberspace' submitted to OEWG (2021) at 7.

[49] Compendium, 72–73.

[50] 'International Law Applied to Operations in Cyberspace'. Paper shared by France with the Open-ended working group established by resolution 75/240, at 4.

[51] Compendium, 90–91.

(do these exceptions apply for both the *sommation* and notification requirements?). The US mentions only the requirement to call upon fulfilment by the responsible state of its obligations and permits derogation from this requirement to preserve the injured state's right — a position which contradicts Article 52(2) of ARSIWA.

There are several possible explanations for this range of positions expressed by states (to set aside the probability that states omitted an analysis of procedural requirements while preparing their submissions for some technical reasons or because they considered them insignificant).

Potentially, states do not consider procedural requirements stipulated by ARSIWA applicable in the cyber context due to its specific nature. Thus, *lex specialis* might be required to define the pre-requisites for responding to malicious cyber operations by countermeasures. Policy arguments to support such *lex specialis* may include indication of the special covert and sensitive nature of cyber capabilities can be revealed by prior notification of countermeasures, especially if they are themselves of cyber nature.[52] Moreover, such notification can make the countermeasures meaningless or quite weak one.[53] One more possible reason is that cyber incidents may be ongoing and high speed, and notification exception can be introduced to procure the possibility of a timely response. Also, it is sometimes considered that public warnings that malicious activities in cyberspace are unacceptable and will lead to countermeasures usually have no effect on 'hostile states such as Russia and China', thus, 'this exception has the potential to become the norm'.[54] It seems that despite the general attractiveness of the idea to develop *lex specialis* for the use of countermeasures in cyberspace, given its specific nature, the lowering of procedural conditions for this means of response carries significant risks, first of all — the danger of escalation, potentially in both cyber and kinetic domains. Moreover, as pointed out by Brazil, there is an increased risk of responding against an innocent actor, as

[52] J. Wright. Attorney General of the United Kingdom, in his speech 'Cyber and International Law in the 21st Century' (23 May 2018) did not agree states are always legally obliged to give prior notice before taking countermeasures against wrongdoing states, and that it would 'not be right for international law to require a countermeasure to expose highly sensitive' defense capabilities.

[53] Compendium, 72–73.

[54] Deeks A. Defend Forward and Cyber Countermeasures. Hoover Working Group on National Security, Technology, and Law. Aegis Series Paper No. 2004. 2020. Available at: www.lawfareblog.com/defend-forward-and-cyber-countermeasures (accessed: 01.07.2024)

cyber operation can be designed to conceal the offender, and the waiver of procedural requirements (particularly, the *sommation*) precludes the possibility for such an actor to validate its lawful conduct.

Another possible explanation is that states do not assume the need to develop *lex specialis*, but rather, most of them did not consider it possible at all to determine as of the date of their contributions the procedural requirements for countermeasures to be applied in the cyber context. In that case, it remains to join Canada's aspirations states practice will further clarify the exact procedural limits of countermeasures as a lawful response to malicious activities in cyberspace.[55]

As an interim summary of what has been discussed above, it can be noted that applicability of the law of state responsibility, including countermeasures, is generally accepted by those states which have expressed their position on the matter, except for China which questions the binding character of ARSIWA, and Brazil which hesitates rules relating particularly to countermeasures are of customary nature. Similarly, there is sufficient consistency in states' positions regarding the fundamental preconditions for countermeasures (the cyber operation should constitute an internationally wrongful act and be attributed to the wrongdoing state), as well as major substantial requisites of lawful countermeasures in response to cyber incidents (they should be addressed to the wrongdoing state, be proportionate, non-forcible, compliant with international law, including *jus cogens*).

Contrary to the general agreement on these points, there is little clarity on the procedural pre-requisites applicable to countermeasures as a response to cyber operations. Article 52 of ARSIWA vests two major requirements on the state intending to take countermeasures: (i) to call upon the responsible state to comply with its obligations, which aims to give this state a chance to evaluate its conduct and, if necessary, to correct it; and (ii) to notify the responsible state of the decision to take countermeasures and offer to negotiate. Review of states' positions revealed particularly a lack of consensus regarding the 'urgent countermeasures' in the cyber context. Although the position expressed, in particular by Italy, on the possibility of waiving both the *sommation* and notification requirements in cases of emergency is understandable from a political standpoint, its expansion can generate dangerous uncertainty. Reports of Special Rapporteur James Crawford on state responsibility demonstrate hot debates on the procedural

[55] Government of Canada. International Law applicable in cyberspace, para 34-36.

requirements to countermeasures during the work of ILC.[56] The requirement of *sommation* is considered by the Special Rapporteur as classical, reflecting a general practice and confirmed by Arbitral Tribunal in the *Air Service Agreement* and by ICJ in the *Gabčíkovo-Nagymaros Project*.[57] Taking into account that the injured state makes a decision on countermeasures based on its sole assessment of the other state, the *sommation* requirement serves a safeguard against an unlawful and premature resort to countermeasures, and their potential misuse. In this sense, application of the 'urgency exception' to the *sommation* requirement, and not only to the prior notification, should not become a 'new norm' for cyber-related countermeasures.

3. Collective Cyber-Related Countermeasures Under International Law

3.1. Drafting History of Article 54 ARSIWA: from Bilateral Model to the 'Saving Clause'

Two articles of ARSIWA, Article 48 and Article 54, deal directly with situations when a non-injured state can invoke state responsibility. Article 48(1) provides for the invocation of responsibility by a non-injured state if the obligation breached protects a collective interest of a group of states including that state, i.e. obligation *erga omnes partes,*[58] *or if the obligation breached is owed to the international community as a whole, i.e. obligation erga omnes.*[59] Thus, in both cases the state invoking responsibility acts not in its individual capacity as an injured party, but in the collective interest — either, of a group of states or the international community.[60] Para (2) of Article 48 specifies the claims available to the non-injured state in these cases: to request from the wrongdoing state cessation of the internationally wrongful act, and reparation. The list of remedies is exhaustive,[61] and it does not include countermeasures.

Article 54 in Chapter II of ARSIWA on countermeasures addresses specifically measures taken by non-injured states. It provides for the right of

[56] J. Crawford, Special Rapporteur. Fourth Report on State Responsibility. 2001. UN Doc. A/CN.4/517, para 67.

[57] Ibid. Para 69.

[58] ARSIWA w. Commentaries, commentary 6 to Art. 48.

[59] Ibid. Commentary 8 to Art. 48.

[60] Ibid, Commentary 1 to Art. 48.

[61] Ibid, Commentary 11 to Art. 48.

any state which is entitled to invoke state responsibility under Article 48 (1) to take 'lawful measures' against that wrongdoing state 'to ensure cessation of the breach and reparation in the interest of the injured state or of the beneficiaries of the obligation breached'.[62] The term 'lawful measures', rather than 'countermeasures', was incorporated deliberately in order 'not to prejudice any position concerning measures taken by states other than the injured state',[63] and thus to include acts of retorsion.

The origins of such a cautious approach can be traced in the convoluted drafting history of ARSIWA. The early drafts were based on the distinction proposed by Special Rapporteur Ago between 'international crimes', i.e. the serious breach of particular obligations most important for the international community, and 'international delicts', i.e. breach of other obligations.[64] The allocation of particular wrongdoings to the category of international crimes could justify collective reaction[65] and give the green light to third-party countermeasures, especially if the notion of an 'injured state' included all states when a wrongdoing by a state constituted an international crime.[66] However, the first reading of Article 40 [1996] on the notion of 'injury' was based on the traditional bilateral model of enforcement. That was strongly opposed by Special Rapporteur Crawford who noted that 'here is no longer (if there ever was) any a priori reason to reduce all relations of responsibility to the form of a bilateral right-duty relation of two states'.[67] Crawford proposed to consider a state injured by a breach of a multilateral obligation if the obligation in question is an obligation *erga omnes* or *erga omnes partes*, and, herewith, the breach specifically affects the state, or 'necessarily affects' the enjoyment by that state of its rights or the performance of its obligations.[68] This distinction, according to Crawford, was to determine the

[62] Art 54 ARSIWA.

[63] ARSIWA w. Commentaries, commentary 7 to Art. 54.

[64] Ibid, 74.

[65] Ibid, 79.

[66] W. Riphagen, Special Rapporteur. Fifth Report on the Content, Forms and Degrees of International Responsibility. 1984. UN Doc. A/CN. 4/380 at 3, Art. 5; Sixth Report on (1) the Content, Forms and Degrees of State responsibility, and (2) the 'Implementation' (mise en oeuvre) of International Responsibility and the Settlement of Disputes, at 5–8 (for commentary to his draft Art. 5).

[67] J. Crawford, Special Rapporteur. Fourth Report on State Responsibility. 2000. UN Doc. A/CN.4/507, 29, para 84.

[68] Ibid. 39, formulation of draft art 40 bis 'Right of a State to invoke the responsibility of another State'.

right of the state to invoke responsibility of another state for a breach of a multilateral obligation: any state party to such an obligation could take countermeasures 'at the request and on behalf' of a state directly injured by the breach (if there was such a directly injured state).[69] In cases of serious breaches of an obligation *erga omnes*, any state could take countermeasures to the extent necessary 'to ensure the cessation of the breach and reparation in the interests of the victims'.[70] It is in this latter case that the model of bilateral interaction between the wrongdoing and the victim-states was replaced by the use of collective, or solidarity, measures [Koskenniemi M., 2001: 346].

Crawford's conception of different categories of 'injured states' and corresponding right to take countermeasures in case of a breach of collective obligations raised hot debates in the ILC and the Sixth Committee. The main concerns of those opposing to the right of states to take countermeasures in response to a breach of *erga omnes* obligations laid in the fears of abuse by powerful states of this right[71] as well as intervention in competence of the UN Security Council to address situations of the most serious breaches of collective obligations.[72] Thus, the final wording of Article 54 of ARSIWA as a 'saving clause' appears to be a necessary compromise after the ILC established that at the time of drafting ARSIWA customary international law did not contemplate the right of states to take countermeasures in the general or collective interest.[73]

One might wonder, to which extent the practice of the International Court of Justice has been influencing the long-years discussion of collective countermeasures in the ILC and its drift between the models of bilateral and collective enforcement in the cases when communitarian norms are breached. In fact, the concept of collective countermeasures has not been much discussed by the ICJ with a remarkable exception of the *Nicaragua* case in which the Court examined whether the support provided by the US to *contras* can be justified as a third-party countermeasure against Nicaragua

[69] Ibid. 108, formulation of draft art 50A 'Countermeasures on behalf of an injured State'.

[70] Ibid. 108–109, formulation of draft art 50B 'Countermeasures in cases of serious breaches of obligations to the international community as a whole'.

[71] UN Doc. A/C.6/55/SR.18, at 11, para 59–62 (Cuba); UN Doc. A/C.6/55/SR.15, at 5–6, para 29, 31 (India).

[72] ILC, Summary Records of the Meetings of the Fifty-Third Session 23 April — 1 June and 2 July — 10 August 2001, 2001 YILC, Vol. I, at 41 para 49.

[73] ARSIWA w. Commentaries, commentary 6 to Art 54.

which supported armed rebels in Costa Rica, El Salvador and Honduras.[74] The Court was firm in its conclusion only victim-states (i.e. Costa Rica, El Salvador and Honduras) could apply countermeasures and not the US as a third party in that situation.[75] At the same time, the ICJ in a manner left the door ajar by saying that 'a use of force of a lesser degree of gravity [than an armed attack] cannot produce any entitlement to take collective countermeasures involving the use of force'.[76] This gave commentators the grounds to suggest that the Court considered collective countermeasures potentially justifiable if taken in response to a grave violation of an *erga omnes* obligation [Dawidowicz M., 2017: 71] and created a sort of an 'echo camera' with the corresponding discussion in the ILC.

3.2. Collective Countermeasures in Cyberspace: To Be or Not to Be

Rule 24 of the Tallinn Manual 2.0 stipulates only the victim-state may apply countermeasures. Herewith, the accompanying commentary to Rule 24 indicates that there was some disagreement among the experts on the permissibility for a non-injured state to apply countermeasures: some of them left such possibility open, provided that the injured state requests assistance; the majority, however, noted with a reference to the *Nicaragua* case that 'countermeasures taken on behalf of another state are unlawful'.[77] The latter group was also divided over whether the non-injured state can assist the injured state in its countermeasures — thus, on the possibility of solidarity measures, and not third-party countermeasures in a narrow sense. Some experts equated the assistance to a victim-state and third-party countermeasures which makes such helping illegal.[78] Others, on the contrary, differentiated the assistance to take countermeasures and taking them on behalf of another state, which means that helping in legal countermeasures is legal itself.[79] Finally, some experts proposed to evaluate solidarity measures for compliance with the obligations owed by the assisting state to the wrongdoing state: if the activities that make up the assistance (e.g.,

[74] Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), Merits, Judgment of 27 June 1986. ICJ Rep. at 127, para 248.

[75] Ibid. 127, para 249.

[76] Ibid.

[77] Tallinn Manual 2.0, commentary 7 to Rule 24.

[78] Ibid. Commentary 9 to Rule 24.

[79] Ibid.

instructions or technical help on hacking-back) violate obligations of the assisting state to the responsible state, such assistance in unlawful.[80] The diversity of views among the experts — authors of the Tallinn Manual 2.0 indicates, inter alia, that there were (and still remain) legal and political arguments both for and against permissibility of collective and/or third-party countermeasures in the cyber context.

This brings us, first, to the analogy of collective self-defence, the right to which is contemplated by Article 51 of the UN Charter as a measure until the Security Council effects its reaction on the threat to the international peace and security. This analogy, however, could justify only third-party countermeasures at the request of the injured state, if the requirements developed in respect of the application of Article 51 to the 'real world' armed conflicts could be transferred into cyberspace with a qualification of a cyber operation as an armed attack.

Another approach could be to justify collective countermeasures as a means to defend collective interest in cyberspace. This, first, requires identifying collective obligations that can be breached by cyber operations. It appears that the known episodes of malicious use of ICTs do not violate the traditional *erga omnes* obligations enlisted by the ILC, such as prohibition of aggression and genocide, protection from slavery and racial discrimination, the right of peoples to self-determination.[81] Identification of a cyber-specific community interest is sometimes suggested in the literature, for instance, the obligation to protect the 'public core of the internet' [Roguski P., 2020: 37–40]. No less important is the question of whether protection of such collective interest (if it is established for the cyber context) a priori justifies its enforcement by third-party countermeasures. It appears that international law in its present state does not contemplate such automatic standing, and clarification on this issue has yet to be developed in the state practice which will depend, in particular, on the inclination towards a bilateral or collectivist model of enforcement.

Alternatively, the permissibility of third-party countermeasures can be supported by a political, rather than purely legal, argument that the malicious cyber-enabled activities should not go unanswered if the victim-state is unable to take countermeasures on its own, in particular due to its low cyber capabilities. In other words, the injured state should not be left alone in a situation of hostile actions in cyberspace. This line of argumentations

[80] Ibid.

[81] ARSIWA w. Commentaries, commentary (9) to Art. 48.

seems to be configuring the position of Estonia who is to date the main advocate for the legality of third-party and collective countermeasures. In her speech on the annual Cyber Conference of NATO Cooperative Cyber Defence Centre of Excellence in May 2019, then-president of Estonia, Kersti Kaljulaid, stressed the importance for the non-injured states to be able to take countermeasures 'to support the state directly affected by the malicious cyber operation'.[82] Later Estonia has reaffirmed its position in the Compendium: 'If a cyber operation is unfriendly or violates international law obligations, injured states have the right to take measures such as retorsions, countermeasures or, in case of an armed attack, the right to self-defense. These measures can be either individual or collective'.[83] Thus, Estonia supports collective and third-party countermeasures as a means of response to malicious cyber operations.

At the same time, there are quite convincing arguments against such an approach. First, granting the states not directly affected by a cyber-attack the right to respond to it by means of countermeasures could open the way to widespread abuse of that right and the emergence in powerful states of a sense of self as the world cyber police. Second, as rightly pointed out by Brazil,[84] whose position has already been cited above, the difficult task of the attribution of a cyber-attack to a state and overall covert nature of cyber operations raise the risk of ill-founded measures against a clean handed state (and, consequently, the risk of invocation of responsibility of the state applying countermeasures). Finally, the significant risk of escalation, potentially spreading to the kinetic domain, due to the high speed of cyber actions proceeding, should be taken into account.

These considerations, perhaps, may explain the more restrained position of the states, other than Estonia, that expressed their attitude towards collective countermeasures in cyberspace. France unambiguously stated that collective countermeasures are not authorised by international law, and therefore France considers itself entitled to take countermeasures only if it is a victim to malicious cyber actions and not in response to violation

[82] K. Kaljulaid, President of the Republic at the opening of Cy Con 2019. Speech in Tallinn. 29 May 2019. Available at: www.president.ee/en/offiial-duties/speeches/15241-president-of-the-republic-at-the-openingof-cycon-2019/index.html (accessed: 05.07.2024)

[83] Estonian positions on 2021-25 United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. 2021, 16.

[84] Compendium, 22.

of another state's rights.[85] Canada seems to be hesitating: on the one hand, it underlines the absence of sufficient state practice or *opinio juris* to answer in affirmative that collective cyber countermeasures are permitted under international law; on the other hand, it recognizes the possibility of technical or legal assistance to the victim-state if the latter does not possess necessary capabilities for a response.[86] Herewith, Canada does not address the issue of qualification of such assistance as third-party countermeasures and its legality under international law.

Overall, the number of states that have expressed their position on the admissibility of collective countermeasures in the cyber domain is too limited to conclude on the support or denial by the international community of this means of reaction to cyber operations. Having said that, one can make an assumption of an increase in the number of supporters of collective cyber countermeasures in the future, not only (or not so much) due to the development of international law in this area, but rather as part of the general trend of uniting the efforts of states to bring trouble-makers in cyberspace to responsibility. Thus, as the next section appeals to the toolbox of economics, namely game theory, — to assess the arguments for and against countermeasures as a potential collective response to cyber operations beyond the purely legal discussion but taking into account also current political processes and incentives for states to act in a particular way.

3.3. Application of Game Theory as an Auxiliary Means to Assess the Applicability of Collective Countermeasures in Cyberspace

The section seeks to provide an additional lens in the form of methodology from the discipline related to international law, namely economics, in order to create a more comprehensive view of the reasons why states are willing to cooperate in their responses, or conversely, refrain from such cooperation. Game theory — the 'study of mathematical models of conflict and cooperation between intelligent rational decision-makers' [Myerson R.B., 1991: 1] — appears to be an adequate tool for developing a stereoscopic view of the motivation for states to unite or disunite in their response to new threats, including cyber-related ones.

---

[85] International Law Applied To Operations In Cyberspace, Paper shared by France with the Open-ended working group established by resolution 75/240. Available at: https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf, at 4 (accessed: 06.07.2024)

[86] Government of Canada. International Law applicable in cyberspace, para 37.

A game-theoretical analysis has been widely addressed in the international relations literature and, more recently, in the literature on international law [Ohlin J. D., 2011]. The tools of game theory are employed as a part of a beyond-positivistic approach to answering the question of why states obey international law [Tesón F., 1998: 74–76]; [Chinen M.A., 2001]; [McAdams R.H., 2009]; [Konyukhovskiy P.V., Holodkova V.V., 2017].

Assuming that states are rational actors that seek to maximize payoffs and reduce costs, cooperation in the cyber security sphere would be mutually beneficial for states wishing to protect their interests in cyberspace. From the standpoint of rational choice doctrine, states tend to cooperate due to the payoffs underlying such cooperation even in the absence of international treaties [Guzman A., 2008: 26]. In certain cases states use the informal instruments to reassure their willingness to cooperate — as, for instance, declaration of alignment of third countries (particularly, EU Candidate Countries Turkey, North Macedonia, Montenegro and Albania; Bosnia and Herzegovina; EFTA States Iceland and Norway and EU Associates Ukraine and Georgia) with EU cyber-related sanctions,[87] or declaration by the EU of solidarity with the US on the impact of the Solar Winds cyber operation.[88] As a step further, formal international agreements are executed such as the Malabo Convention. In light of coordination games theory (that are games which contemplate coordination of players' actions to achieve the goals of their cooperation), agreements serve to formalize arrangements between the parties and increase stability of the agreed regime on complicity, especially in the situation when the incentives for informal cooperation may weaken over time. In other words, international treaties apparently facilitate cooperation of states in a coordination game in the setting of uncertainty about the players' payoffs in the future [Guzman A., 2008: 26, 28].

The rational choice assumption provides various avenues for the analysis not only of the incentives for states to cooperate and comply with obligations under international agreements, but also the application of counter-

[87] The text of the declaration is available at: www.consilium.europa.eu/en/press/press-releases/2020/06/19/declaration-by-the-high-representative-on-behalf-of-the-eu-on-the-alignment-of-certain-third-countries-concerning-restrictive-measures-against-cyber-attacks-threatening-the-union-or-its-member-states/# (accessed: 06.07.2024)

[88] Council of the EU. Declaration by the High Representative on behalf of the European Union Expressing Solidarity with the United States on the Impact of the Solar Winds Cyber Operation.

measures as strategic interaction. Such situations of strategic interaction between the players, or 'games', are divided in a number of classes.

The interaction 'cyber operation — reaction' can be qualified as a cooperative game. States as game players are bound, at least in theory, with the commitments enforced under international law, including the principles of sovereignty and non-interference in the internal affairs of other states. As these commitments can be enforced through outside parties, the game is deemed cooperative.[89] In non-cooperative games, although players can cooperate with each other, any cooperation must be self-enforcing.[90] Cooperative game theory contemplates forecasting coalitions that the players will form, their collective actions and group payoffs. In non-cooperative theory, a game is a detailed model of various moves available to the players, the analysis of individual payoffs and Nash equilibria.[91] In a cooperative game, players other than the state applying countermeasures and the target can join the game at each decision stage, at their discretion, as 'white knights' in cooperation with the applicant of the countermeasures or 'black knights' on the side of the designated wrongdoer [Eyler R., 2008: 37]. Each episode of the application of countermeasures undermines reputation of the target as an actor that complies with the undertaken commitments. A bad reputation of a state violating its international obligations raises costs for this state in future cases of cooperation, not only in that particular game, but also other scenarios of cooperation with different players [Guzman A., 2008: 34–35]. In this sense, the retaliatory role of countermeasures correlates with the reputational damage effect that complicates for the target process of cooperation with other players and increases its cost.

Conclusion

The paper has examined collective, or third-party, countermeasures as a potential means of response to malicious cyber-enabled conduct of a state. An analysis of state positions reveals almost complete agreement on general

[89] Non-Cooperative Game. Dictionary of Game Theory Terms, Game Theory.net. Available at: www.gametheory.net/dictionary/Non-CooperativeGame.html (accessed: 06.07.2024)

[90] Ibid.

[91] Cooperative Game Theory: Characteristic Functions, Allocations, Marginal Contribution. 2007. Available at: https://web.archive.org/web/20160527184131if_/http://www.uib.cat/depart/deeweb/pdi/hdeelbm0/arxius_decisions_and_games/cooperative_game_theory-brandenburger.pdf, 1 (accessed: 06.07.2024)

applicability of the law of state responsibility, including countermeasures, in cyberspace, but a lack of clarity on the procedural pre-requisites applicable to the countermeasures as a response to cyber operations. Appeal to the drafting history of ARSIWA has shed light on a shift from the traditional bilateral model of enforcement to the collective, or solidarity, measures and, finally, to a 'saving clause' as a necessary compromise within the drafters. Development of inter-state relations demonstrates states overall willingly cooperate to increase reputational, political and economic pressure for malicious actions in cyberspace. The cooperation has so far taken the forms of collective accusations and collective economic sanctions. At the same time, several states (the US in the first stance) demonstrate the desire to expand the toolbox of measures applied collectively to respond to malicious cyber incidents, regardless of their legal qualification. Returning to the hypothesis posed at the beginning of this study, it is now possible to conclude that states may be willing to join in the application of such measures, driven by the considerations of rational choice and (or) conditions of being in an alliance or a coalition of 'like-minded' states. The use of collective countermeasures, thus, may at some point become a logical step towards increasing the joined efforts of states, including within the framework of alliances, to counter cyber incidents.

References

1. Chinen M. A. (2001) Game Theory and Customary International Law: A Response to Professors Goldsmith and Posner. *Michigan Journal of International Law*, vol. 23, no. 1, pp. 143–189.

2. Coco A., Dias T. and van Benthem T. (2022) Illegal: The Solar Winds Hack under International Law. *European Journal of International Law*, vol. 33, no. 4, pp. 1275–1286.

3. Corn G. and Jensen E.T. (2018) The Use of Force and Cyber Countermeasures. *Temple International & Comparative Law Journal*, no. 32, pp. 127–136.

4. Danielsen D. (2016) International Law and Economics: Letting Go of the "Normal" in Pursuit of An Ever-Elusive. In: Orford A. and Hoffmann R. (eds.) The Oxford Handbook of the Theory of International Law. Oxford: University Press, 1045 p.

5. Dawidowicz M. (2017) *Third-Party Countermeasures in International Law*. Cambridge: University Press, 438 p.

6. Delerue F. (2020) *Cyber Operations and International Law.* Cambridge: University Press, 513 p.

7. Finnemore M. and Hollis D. B. (2020) Beyond Naming and Shaming: Accusations and International Law in Cybersecurity. *European Journal of International Law*, vol. 31, no. 3, pp. 969–1003.

8. Eyler R. (2008) *Economic Sanctions: International Policy and Political Economy at Work*. N. Y.: Palgrave MacMillan, 251 p.

9. Guzman A. (2008) *How International Law Works: A Rational Choice Theory*. Oxford: University Press, 260 p.

10. Haataja S. (2020) Cyber Operations and Collective Countermeasures under International Law. *Journal of Conflict and Security Law*, vol. 25, no. 1, pp. 33–51.

11. Henriksen A. (2015) Lawful State Responses to Low-Level Cyber-Attacks. *Nordic Journal of International Law*, vol. 84, no. 2, pp. 323–351.

12. Huang Z., Ying Y. (2021) Chinese Approaches to Cyberspace Governance and International Law in Cyberspace. In: N.Tsagourias and R. Buchan (eds.) Research Handbook on International Law and Cyberspace. 2nd ed. Cheltenham: Edward Elgar Publishing, 634 p.

13. Keshner M.V. (2015) Collective countermeasures taken against the Russian Federation: the issue of legitimacy. *Russian Law Journal,* vol. 101, no. 2, pp. 32–38 (in Russ.)

14. Keshner M.V. (2015) *Economic sanctions in the modern international law*. Moscow: Prospekt, 184 p. (in Russ.)

15. Keshner M.V. (2017) *Law of international responsibility*. Moscow: Prospekt, 240 p. (in Russ.)

16. Kononova K.O. (2010) 'Collective countermeasures': a question on the legitimacy of their existence and the vector of development in international law in the 21th century. *Mezhdunarodnoe publichnoe i chastnoe pravo*, no. 6, pp. 13–16 (in Russ.)

17. Konyukhovskiy P.V. and Holodkova V.V. (2017) Application of Game Theory in the Analysis of Economic and Political Interaction at the International Level. *Contributions to Game Theory and Management*, no. 10, pp. 143–161.

18. Koskenniemi M. (2001) Solidarity Measures: State Responsibility as a New International Order? *British Yearbook of International Law*, vol. 72, no. 1, pp. 337–356.

19. Kozheurov Ya.S. (2015) The War of "Sanctions" and the Law of International responsibility. *Russian Law Journal*, vol. 101, no. 2, pp. 179–182 (in Russ.)

20. Lahmann H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defense, Countermeasures, Necessity, and the Question of Attribution*. Cambridge: University Press, 326 p.

21. Lipkina N.N. (2013) Countermeasures and sanctions as means of ensuring of the implementation of international obligations. *Law, Legislation, Person,* vol. 17, no. 2, pp. 48–55 (in Russ.)

22. Lukashuk I.I. (2004) *Law of international responsibility*. Moscow: Wolters Kluwer, 405 p. (in Russ.)

23. McAdams R.H. (2009) Beyond the Prisoner's Dilemma: Coordination, Game Theory, and Law. *Southern California Law Review*, vol. 82, no. 2, pp. 209–258.

24. Myerson R.B. (1991) *Game Theory: Analysis of Conflict*. Harvard: University Press, 568 p.

25. Ohlin J.D. (2011) Nash Equilibrium and International Law. *Cornell Law Review*, vol. 96, pp. 869–899.

26. Roguski P. (2020) Collective Countermeasures in Cyberspace — Lex Lata, Progressive Development or a Bad Idea? 12th International Conference on Cyber Conflict. DOI: 10.23919/CyCon49761.2020.9131715.

27. Roscini M. (2014) *Cyber Operations and the Use of Force in International Law.* Oxford: University Press, 307 p.

28. Schmitt M.N. (ed.) (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: University Press, 598 p.

29. Rusinova V., Assaf A., Moshnikov D. (2020) Dispute on sovereignty in cyberspace: content, limits, and prospects for the development of positivistic discourse. *International Justice*, vol. 19, no. 3, pp. 55–66 (in Russ.)

30. Schmitt M.N., Watts S. (2021) Collective Cyber Countermeasures? *Harvard National Security Journal*, no. 12, pp. 373–411.

31. Shany Y., Schmitt M.N. (2020) An International Attribution Mechanism for Hostile Cyber Operations. *International Law Studies*, vol. 96, pp. 196–222.

32. Tesón F. (1998) *A Philosophy of International Law*. New York: Routledge, 208 p.

33. Tsagourias N. (2015) The Law Applicable to Countermeasures against Low Intensity Cyber Operations. *Baltic Yearbook of International Law Online*, no. 14, pp. 105–123.

34. Watts S. (2015) Low-Intensity Cyber Operations and the Principle of Non-Intervention. In: Ohlin J., Govern K. et al. (eds.). Cyber War: Law and Ethics for Virtual Conflicts. Oxford: University Press, 320 p.

Information about the author:

E.A. Martynova — Cyber BRICS Fellow.

The article was submitted to editorial office 07.08.2024; approved after reviewing 30.08.2024; accepted for publication 05.09.2024.