Palacký University in Olomouc
Faculty of Law

Jakub Spáčil

Non-forcible Unilateral Remedies to Cyber Operations: Retorsion, Plea of Necessity and Countermeasures

Rigorous Thesis

Olomouc 2024

I would like to dedicate this work to my family and friends, especially my mother Iva and her husband Pavel, my grandparents Jitka and Vojtěch and my sister Barbora.

I would also like to thank prof. JUDr. Dalibor Jílek, CSc. for his expert guidance and support and my close friend JUDr. Adam Talanda, Ph.D. for being my academic role model.

I hereby declare that I have written this rigorous thesis on Non-forcible Unilateral Remedies to Cyber Operations: Retorsion, Plea of Necessity and Countermeasures independently and I have cited all sources used. I further declare that the actual text of this thesis, including footnotes, is 188 143 characters including spaces.

In Olomouc 28. 5. 2024 Jakub Spáčil

Table of Contents

Introduction

"Watch closely as grandpa topples an empire by changing 1 to a 0", a mad scientist Rick Sanchez turns to his grandchildren in the American TV show *Rick and Morty* just before he changes the value of the intergalactic empire's currency from 1 to 0 in the computer system, thus dismantling the entire social structure of this interplanetary entity.[1]

Although the above series is full of bizarreness and exaggeration, the moment described above demonstrates with dangerous accuracy how terrestrial society is also dependent on modern technology including computers and networks and how vulnerable this dependency makes it.

The origins of the Internet as we know it today can be traced back to the ARPANET system, which was developed in 1969. However, it was the mass proliferation of personal computers, and subsequently the Internet, in the 1990s, that made the network for exchanging information between universities a phenomenon that changed the world and the lives of literally everyone on the planet. In 2024, a staggering 5,35 billion people (66 % of the world's population) have access to the Internet[2] and by 2030 this number is expected to reach 7,5 billion (90 % of the world's population).[3]

The Internet raises the standard of living, it is a means of spreading education, an effective work tool, a source of entertainment. It permeates almost every moment of our lives, from the morning podcast streamed in the shower, to traffic updates on the way to work, to an evening "Netflix and chill" with our favourite show.

Like any powerful instrument, however, the Internet has its downsides. Drug trafficking, prostitution, child pornography, money laundering or even murder for hire. These services can also be found on the Internet, often in a hidden part of it known as the Dark Net. They are often operated by organised transnational criminal groups, but active individuals are no exception. Dark Net-related activities are often illegal and therefore have an obvious legal overlap, which, particularly in the case of transnational crime, also has a strong international legal aspect.

However, in this paper we will not be concerned with the role of the Internet in the life of the individual or society, whether it is positive or negative. We are interested in its role and the role of

---

[1] CARTOON NETWORK STUDIOS. *Rick and Morty: The Rickshank Rickdemption*. Burbank, USA: Cartoon Network Studios, 2017 [online]. [viewed 14 May 2024] Available from: https://www.youtube.com/watch?v=mweTc7tDO3I&ab_channel=AlephNull.

[2] KEMP, S. Digital 2024: Global Overview Report. *Datareportal.com* [online]. 31 January 2024 [viewed 14 May 2024]. Available from: https://datareportal.com/reports/digital-2024-global-overview-report.

[3] MORGAN, S. Top 10 Cybersecurity Predictions And Statistics For 2024. *Cybersecurityventures*.com [online]. 5 February 2024 [viewed 14 May 2024] Available from: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/.

cyberinfrastructure in general in the "life" of states as primary subjects of international law. Indeed, in this area too, the development of technology, especially computer networks (i.e. not only the Internet) and computers as such, has brought about a medium-sized revolution.

Starting with the cyber attack on Estonia in 2007, it became clear to national leaders that cyberspace and cybersecurity were terms that would be at the top of their vocabularies for a long time. States have gradually realised that their growing dependence on cyberinfrastructure, which has newly permeated critical areas such as energy, banking and healthcare, is a significant security risk. Other states, on the other hand, have realized that this may be an opportunity to negatively impact states with which they would not have a chance to succeed in a conventional military confrontation.

For the last fifteen years, we have been witnessing a cyber arms race, where the more technologically advanced states in particular are trying to protect their own cyber infrastructure (building defensive capacity) on the one hand, and on the other hand they are also building offensive capacity, either for the purpose of active defense or for potential use against the enemy in (possibly military) conflict.[4]

Wherever there is interaction between two or more states, including in cyberspace, international law plays a role. And in the case of cyber operations, it is no different. The gradual development of international law over several hundred, if not thousands, of years has led to the emergence of rules that states recognize and respect. These rules vary to some extent on land, at sea, in the air and in space. Cyberspace, then, can be considered a new area in which international law needs to be applied, and which has its own specificities (e.g., the absence of borders or a material substrate). However, the speed of technological development does not give the international community the luxury of several centuries of development to allow new rules regulating the conduct of states (and other subjects of international law) to emerge through a lengthy customary-law-forming process. Rules for the conduct of states in cyberspace had to be developed much more quickly because cyberspace exists and is a place of interaction between states regardless of the readiness of international law norms.

The basic international legal framework was established mainly thanks to the work of the United Nations Groups of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, which between 2005 and 2021 formulated the elementary rules for the application of international law in

[4] CRAIG, A., VALERIANO, B. Conceptualising Cyber Arms Races. In: PISSANIDIS, N., RÕIGAS, H., VEENENDAAL (eds.). *2026 8th International Conference on Cyber Conflict*. Tallinn: NATO CCDCOE Publications, 2016, p. 141 – 158.

cyberspace.[5] The outcome of their work was, inter alia, the conclusion adopted by the United Nations General Assembly that international law is applicable in cyber space.[6] However, the resolution of this primary question, the general applicability of international law in cyberspace, led to a new debate - how should existing rules of international law be applied in cyberspace? And it is this question that is the leitmotif of the text you are now reading.

Scholars and legal practitioners have been working intensively on the application of the various instruments of international law in cyberspace for more than a decade producing *inter alia* seminal books created under the leadership of Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare (published 2013) and Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (published 2017). However, given the nature of international law, which is largely dependent on state practice for its creation and interpretation, it is certainly not possible to rely solely on academic literature. An important source of information on the application of international law in cyberspace are also the so-called "national positions", the official positions of states on the application of international law in cyberspace.[7] These main sources are then, of course, complemented by hundreds and thousands of scholarly articles published across continents.

Although considerable attention has been paid to the application of international law in cyberspace, it is a topic so broad and dynamic that it still provides more than enough room for further research. After all, the Tallinn Manual 2.0 mentioned above defines and comments on 154 rules of international law, each of which could be the subject of a separate book. That is why this thesis focuses on only three instruments of international law that are united by a single idea - they are instruments that can provide a legal basis to justify defensive cyber operations, usually in response to cyber operations carried out by other states or non-state actors from the territory of those states. These instruments are called retorsion, plea of necessity and countermeasures.

While retorsion is an unfriendly act not inconsistent with international law (e. g. expulsion of diplomats), plea of necessity and countermeasures are circumstances precluding wrongfulness, which means that measures falling under these instruments are acceptable even though they would normally constitute a violation of international law, both general and particular, customary and

---

[5] TIIRMAA-KLAAR, H. The Evolution of the UN Group of Governmental Experts on Cyber Issues. *Cyberstability Paper Series: New Conditions and Constellations in Cyber* [online]. December 2021 [viewed 14 May 2024]. Available at: https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf.

[6] UNITED NATIONS. *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. [online]. Doc. A/68/98, 24 June 2013 [viewed 14 May 2024]. Available from: https://documents.un.org/doc/undoc/gen/n13/371/66/pdf/n1337166.pdf.

[7] CYBER TOOLKIT. National positions. Cyberlaw.ccdcoe.org [online]. [viewed 14 May 2024]. Available from: https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions.

treaty-based (e. g. restriction of access to one's own airspace for aircraft of a state responsible for a hostile cyber operation). Individual chapters of this thesis are devoted to a detailed analysis of these instruments and their application in cyberspace.

What is not addressed in this thesis is the attribution of cyber operations. Although this is one of the key issues in relation to cyber operations, the scope of this thesis does not allow for its in-depth analysis. However, legal attribution of the cyber operations of the target state is not a prerequisite for measures taken on the basis of retorsion and plea of necessity, therefore it can be omitted in this context. Nevertheless, the author addresses the issue of attribution in a separate scholarly article.[8]

In relation to terminology, it should be noted that this thesis will often refer to two states, one of which is the victim of a cyber operation and the other of which is either the originator or is connected to the operation (e. g. because the cyber operation was carried out from its territory). The state that is the victim of a cyber operation will be referred to as the *victim state* or *injured state*. The state that is the originator of the cyber operation or is otherwise associated with it, and against which retaliatory measures may therefore be directed, will be referred to as the *responsible state*, *target state* or *territorial state*.

This work is based on two main types of sources - the academic literature and state practice, which is represented mainly by official state positions on application of international law in cyberspace. Sources dating back to the 1990s were considered in the literature review, but the focus was primarily on more recent sources (from 2015 onwards), as many of the issues previously discussed in older literature have been resolved, either by the work of the UN GGE or by the evolving state practice. However, in terms of the usefulness for this text, the national positions published from 2019 to 2023 should be considered as a key source, allowing more or less clear conclusions to be drawn in relation to some problematic aspects of the application of retorsion, plea of necessity and countermeasures in cyberspace (e. g. regarding forcible countermeasures).

The thesis is divided into three chapters according to the three instruments of international law whose application in cyberspace is dealt with. The ordering of the chapters corresponds to the strength of each instrument, which is measured by the potential interference with the rights of the target state. Thus, the first chapter is devoted to retorsion, which does not allow interference with the rights of other states, and measures taken with reference to retorsion will therefore generally be the least invasive (which does not automatically mean that they will be the least effective). The

[8] SPÁČIL, J. Attribution of Cyber Operations: Technical, Legal and Political Perspectives. *International and Comparative Law Review*, 2024, 24 (1) (to be published 2Q 2024).

second chapter discusses the plea of necessity, an institution that allows interference with the rights of other states, but is bound by very strict conditions of application. The third instrument are countermeasures, which will constitute the most significant interference with the rights of target states, but this interference is also justified by the fact that, unlike the previous two instruments, the legal attribution of the original hostile act to the target state is a prerequisite for the adoption of countermeasures. This thesis is a collection of scholarly papers that have been published in peer-reviewed journals, with each chapter corresponding to one scholarly article.[9]

The author asks the following research questions: What are the specific conditions of applicability and limits of the instruments of retorsion, plea of necessity and countermeasures in cyberspace? What specific measures can be subsumed under each instrument and are there any measures specific to cyberspace? Are the academic conclusions expressed in particular in Tallinn Manual 1.0 and 2.0 supported by state practice? What conclusions for the application of these instruments in cyberspace can be drawn from recent state practice?

The main objective of this paper is to further define how the instruments of retorsion, plea of necessity and countermeasures are to be applied in cyberspace, with particular emphasis on recent (2019-2023) state practice.

[9] In accordance with Article 6 (3) of the Řád rigorózního řízení Univerzity Palackého v Olomouci (B1-17/4-HN-ÚZ01).

1 Retorsion: Underrated Retaliatory Measure Against Malign Cyber Operations[10]

1.1 Introduction

When historians describe the second decade of the 21st century, they will undoubtedly consider the spread of almost unlimited access to the Internet and the previously unimaginable interconnection of people and things that it has brought with it as one of the fundamental phenomena that has influenced the development of societies around the world. This technological development has brought many new opportunities and has led to an increase in the standard of living, but it also entails new risks. One of these is malign cyber operations, which can cause consequences ranging from mere inconvenience (temporary inaccessibility of the governmental website), to financial losses (ransomware extortion), to material damage and death (cyber-attack on critical infrastructure).

Cyber operations are not only a problem for the private sphere, but also affect international relations. It is no coincidence that cyberspace is considered the fifth domain of warfare - next to the air, water, ground and space.[11] International relations are regulated by international law, and therefore legal issues are an important part of the cyber defence debate. This article discusses the topic of unilateral remedies to cyber operations, specifically retorsion, which is one of the concepts of international law that has received the least attention[12] despite the fact that it is a term under which the vast majority of unilateral retaliatory measures taken by states against unfriendly or illegal conduct of other states in cyberspace can be subsumed.[13]

The fundamental question of this paper is what role does retorsion play in the current state practice and what specific measures fall into this category and which do not. This questions will be answered

---

[10] This work was originally published in the Baltic Journal of Law & Politics [SPÁČIL, J. Retorsion: Underrated Retaliatory Measure Against Malign Cyber Operations. *Baltic Journal of Law & Politics*, 2023, 17(1)] and won the first place in the faculty round of the competition in Student Scientific and Professional Activities 2023 (SVOČ) and third place in the Czech-Slovak final. Research was supported by the student project "International legal aspects of defense against cyber operations: retorsion and countermeasures" (IGA_PF_2022_004) of the Palacky University. The work was prepared under the supervision of prof. JUDr. Dalibor Jílek, CSc.

[11] von HEINEGG, Wolff Heintschel. Territorial Sovereignty and Neutrality in Cyberspace. *International Law Studies*, 2013, vol. 89, p. 123.

[12] KOSSEFF, J. Retorsion as a Response to Ongoing Malign Cyberoperations. In: JANČÁRKOVÁ, T., LINDSTRÖM, L., SIGNORETTI, M., TOLGA, I., VISKY, G. (eds.). *2020 12th International Conference on Cyber Conflict*. Tallinn: NATO CCDCOE Publications, 2020, p. 15; McDONALD, N. and McLEOD, A. 'Antisocial Behaviour, Unfriendly Relations': Assessing the Contemporary Value of the Categories of Unfriendly Acts and Retorsion in International Law. *Journal of Conflict & Security Law*, 2021, 26(2), p. 423.

[13] DAWIDOWICZ, M. Third-Party Countermeasures in International Law. 1st ed. New York: Cambridge University Press, 2017, p. 29.

through an analysis of state practice, which is central to finding and interpreting international law that is largely unwritten and subject to constant evolution.

1.2 Retorsion as a concept

A state that becomes a victim of a cyber operation (target state) naturally seeks to protect its interests. Its main objective is to eliminate the negative consequences of the cyber operation and prevent its continuation or repetition. If the source of the cyber operation is located on the territory of another state (or is organised by that state), the target state must respect the rules of international law in choosing the means to achieve these objectives and not commit impermissible interference with the sovereignty of another state or violate other rules of international law. If the target state wants to avoid committing an internationally wrongful act in the implementation of cyber defence, the measures it takes must be within the bounds of one of the following four concepts of international law: retorsion, countermeasures, plea of necessity and self-defence.[14] While the latter three concepts constitute so-called circumstances precluding wrongfulness,[15] the nature of retorsion is different.

Retorsion is "unfriendly conduct which is not inconsistent with any international obligation of the state engaging in it".[16] Typical examples of retorsion include protests, denial of access to state resources, economic sanctions or expulsion of diplomats.[17] It is therefore an act that is not prohibited by international law, but will be considered hostile by the state concerned in moral or political terms.[18] When we speak of conduct prohibited by international law, we are referring to any act or omission by which a state would violate its international obligation, whether arising from a treaty or customary law.[19] Retorsion is typically in response to a hostile (but lawful) act by another state, but can also be used to respond to an internationally wrongful act by another state.[20]

---

[14] SCHMITT, Michael, N. et al. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, 2017, p. 82.
[15] INTERNATIONAL LAW COMMISSION. *Yearbook of the International Law Commission: Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*. 2001, vol. II, part two, pp. 71-86 (hereinafter „ARSIWA").
[16] ARSIWA, p. 128.
[17] GIEGERICH, T. Retorsion. In: WOLFRUM, R. (ed.) *Max Planc Encyclopedia of Public International Law*. Oxford: OUP, 2017; BANKS, C. W. The Bumpy Road to a Meaningful International Law of Cyber Attribution. *AJIL Unbound*, 2019, 113(1), p. 194.
[18] McDONALD and McLEOD: *'Antisocial Behaviour…*, p. 425.
[19] McDONALD and McLEOD: *'Antisocial Behaviour…*, p. 425.
[20] Ibid., p. 421; RUYS, T. Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework. In: Herik, L. (ed.) *Research Handbook on UN Sanctions and International Law*. Cheltenham: Edward Elgar Publishing, 2017, p. 24; ARSIWA, p. 128.

Retorsion is not a right. Rather, we need to talk about freedom.[21] As a result, it is not a legal concept, but a descriptive category (or technical term),[22] which has no direct legal effect.[23] Freedom, unlike right, is not limited by conditions.[24] It should be stressed that this lack of limits applies only if the conduct under consideration actually fulfils the defining characteristics of retorsion (unfriendly, but lawful conduct). If the conduct does not bear these characteristics, it is not retorsion and will therefore constitute internationally wrongful act, unless its wrongfulness is excluded by some other instrument of international law (e.g. countermeasures).

Thus, retorsion is limited on the one hand by political and economic considerations that may exclude its factual feasibility (e.g., if the implementation of a hostile act would harm the state's own interests more than the interests of the state concerned),[25] and on the other hand by international law, because although retorsion itself is not regulated by international law,[26] it is the rules of international law that constitute its limit.[27] This is to say that retorsion is, by definition, only legal conduct (conduct not prohibited by international law, conduct not violating an international legal obligation of any kind), and if a state violates a rule of international law by its conduct, such conduct (or omission) cannot be described as retorsion.[28] Typical examples of rules that will preclude the classification of a state's conduct as retorsion are sovereignty or the principle of non-intervention in internal affairs.[29]

Retorsion should be distinguished from "unfriendly act". Retorsion is essentially a qualified unfriendly act, since it is itself a reaction to a previous unfriendly act of the state against which it is directed. It is therefore effectively the same act (e.g. the expulsion of a diplomat), the difference is only in the context.[30] However, for both categories it is true that they are lawful measures.[31]

The absence of regulation of retorsion by international law implies that it is not subject to limitations like other unilateral remedies. Retorsion therefore does not need to be necessary, temporary, reversible or in any manner proportional and it may even contain punitive element.[32] Nor is the state limited in relation to the motive, purpose, duration or character of the measure

---

[21] RUYS: *Sanctions, Retorsions…*, p. 24; DAWIDOWICZ: *Third-Party Countermeasures…*, p. 28.
[22] GRANT, J., P., BARKER, C., J. *Parry & Grant encyclopaedic dictionary of international law*. 3rd ed. New York: Oxford University Press, 2009, p. 525.
[23] McDONALD and McLEOD: *'Antisocial Behaviour…*, p. 424.
[24] RUYS: *Sanctions, Retorsions…*, p. 24.
[25] KOSSEFF: *Retorsion…*, p. 15.
[26] DAWIDOWICZ: *Third-Party Countermeasures…*, p. 28.
[27] McDONALD and McLEOD: *'Antisocial Behaviour…*, p. 441.
[28] KOSSEFF: *Retorsion…*, p. 15.
[29] KOSSEFF: *Retorsion…*, p. 11; R-2, p. 441
[30] McDONALD and McLEOD: *'Antisocial Behaviour…*, p. 427.
[31] Ibid., p. 422.
[32] Ibid., p. 424; RUYS: *Sanctions, Retorsions…*, p. 24; DAWIDOWICZ: *Third-Party Countermeasures…*, p. 28.

chosen.[33] Retorsion may thus justify even measures constituting mere revenge.[34] The question of whether retorsion is justified is not a matter for legal consideration at all.[35] The fact remains that, despite the absence of regulation, states tend to use proportionate measures in order to pursue "just and sound politics".[36] The question is whether, in the case of wholly malicious hostile conduct, this could be an abuse of the law, as Giegerich suggests.[37] The fact is that such conduct would be contrary to the requirement of friendly relations among states.[38] On the other hand, retorsion is not a right, but only a descriptive category, and for this reason alone "abuse of the right" cannot be an apt label for such state action. Moreover, the motive or objective (or lack thereof) is not relevant to the legality of the conduct.[39] Other authors then take the view that retorsion is also limited by the proportionality requirement or the exclusion of improper motive, but these are rather marginal views.[40]

If retorsion is not regulated by law, does it make sense to address it from a legal perspective? It undoubtedly does and for at least two reasons. First, retorsion refers to lawful conduct. If the conduct is not lawful, it is an internationally wrongful act, which gives rise to legal consequences (secondary obligations), unless liability is excluded by circumstances precluding wrongfulness. Therefore, specific retaliatory measures must be accurately identified and subsumed under the correct international law concept. Retorsion thus creates a contrast against which legal and illegal conduct can be distinguished.[41] The second reason why retorsion cannot be left out of the concern of international lawyers is that by using the term retorsion to describe its own conduct, a state signals to the state concerned that it is acting within the bounds of international law, which can have a de-escalatory effect.[42]

The use of the concept of retorsion has its practical implications, advantages and disadvantages. The advantages include the de-escalatory potential rooted in the signaling of lawfulness of adopted measure, the clarification of the "freedom of maneuver" consisting in the clarification of measures

---

[33] KOSSEFF: *Retorsion…,* pp. 15-16; DAWIDOWICZ: *Third-Party Countermeasures…,* p. 28.
[34] SCHMITT, M., N. et al. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. 1st ed. Cambridge: Cambridge University Press, 2013, p. 40.
[35] ANDERSON, T. Fitting a Virtual Peg into a Round Hole: Why Existing International Law Fails to Govern Cyber Reprisals. *Arizona Journal of International & Comparative Law*, 2016, 34(1), p. 144; GRANT, BARKER: *Parry & Grant encyclopaedic dictionary…,* p. 525; DAWIDOWICZ: *Third-Party Countermeasures…,* p. 28.
[36] DAWIDOWICZ: *Third-Party Countermeasures…,* p. 28.
[37] GIEGERICH: *Retorsion…*; SCHMIDT, J. The Legality of Unilateral Extra-territorial Sanctions under International Law. *Journal of Conflict & Security Law*, 2022, 27(1), p. 73.
[38] UN General Assembly Resolution 2625 from 24 October 1970 *("The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States").*
[39] KOSSEFF: *Retorsion…,* p. 16.
[40] SCHMIDT: *The Legality of…*, p. 73; McDONALD and McLEOD: *'Antisocial Behaviour…,* p. 424.
[41] McDONALD and McLEOD: *'Antisocial Behaviour…,* p. 424.
[42] Ibid.

that will generally be considered as retorsion (allowing decision makers to act effectively and legally at the same time) and finally, in the future, the argumentation of retorsion in litigation can be expected.[43] On the other hand, there are risks, the main one being the potential misuse of the concept to illegitimately justify internationally wrongful conduct.[44]

Ruys with reference to the work of White and Abass states that "the issue of enforcement by means of non-forcible measures is and remains 'one of the least developer areas of international law'".[45] One cannot but agree with this conclusion. It applies even more to retorsion than to related concepts. This is evidenced by the complete absence of an analysis of the term in the case law of the International Court of Justice,[46] as well as by the fact that for the time being it received little attention by the group of experts working on the Tallinn Manual 2.0 on International Law Applicable to Cyber Operations, which, although described as "the most comprehensive analysis"[47] on the application of international law in cyberspace, contains only six brief mentions of retorsion (although, for example, countermeasures are the subject of six rules elaborated over 20 pages).[48] One can only hope that the third edition of the Tallinn Manual will already give sufficient attention to this issue.[49]

1.3 Retaliation against cyber operations - analysis of state practice

In recent years, it has been possible to observe the implementation of a number of measures in response to cyber operations, which have had the character of a retorsion. At the same time, the term has also begun to appear relatively widely in the national positions of states on the application of international law in cyberspace. It is to the analysis of these forms of state practice that the next section of the text is devoted.

---

[43] McDONALD and McLEOD: *'Antisocial Behaviour…,* pp. 435-438.
[44] Ibid., p. 440.
[45] RUYS: *Sanctions, Retorsions…*, p. 23.
[46] McDONALD and McLEOD: *'Antisocial Behaviour…,* p. 433.
[47] EUROPEAN PARLIAMENTARY RESEARCH SERVICE. *Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence* [online]. May 2020 [viewed 20 February 2023], p. 2. Available from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI(2020)651937_EN.pdf.
[48] SCHMITT et al: *Tallinn Manual 2.0...* , pp. 112, 118, 131.
[49] The NATO Cooperative Cyber Defence Centre of Excellence. *CCDCOE to Host the Tallinn Manual 3.0 Process* [online]. Ccdcoe.org [retrieved 12 February 2023]. Available from: https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/.

1.3.1 Application of retorsion measures

One of the first examples of major state sponsored cyber operation is the cyber activity directed at Estonian banks and public services in 2007.[50] Among the measures taken by the affected institutions in cooperation with the government was blocking access to certain IP addresses from Russia.[51] As states have sovereignty over cyber infrastructure located on their territory, such action does not constitute a violation of international law and is a retorsion.[52]

Russian intelligence services interfered in the 2016 US presidential election through, among other things, cyber operations.[53] One of these involved the hacking and subsequent publication of the private email communications of presidential candidate Hillary Clinton in order to damage her and increase the chances of Donald Trump's election.[54] The US responded to the election meddling with the expulsion of 35 Russian diplomats.[55] Expulsion of diplomats is a typical example of retorsion.[56] At the same time, technical information on Russian cyberspace activities was released to "identify, detect, and disrupt Russia's global campaign of malicious cyber activities" in the United States and abroad.[57] A series of additional sanctions, at least some of which could be considered retorsion, followed in 2018.[58]

North Korea uses cyber operations mainly to raise funds, but also to protect its interests.[59] Therefore, in 2019, the US adopted sanctions against three groups linked to the North Korean

---

[50] SCHMITT et al: *Tallinn Manual on the International Law Applicable to Cyber Warfare…*, p. 40.
[51] SCHMITT et al: *Tallinn Manual on the International Law Applicable to Cyber Warfare…*, p. 40.
[52] SCHMITT N. M. "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, 2015, 54(1), p. 701.
[53] SANGER, D. E. Obama Strikes Back at Russia for Election Hacking. *nytimes.com* [online]. 29 December 2016 [viewed 23 February 2023]. Available from: https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html.
[54] ABRAMS, A. Here's What We Know So Far About Russia's 2016 Meddling [online]. 18 April 2019 [viewed 23 February 2023]. Available from: https://time.com/5565991/russia-influence-2016-election/.
[55] SAGNER: *Obama Strikes Back…*; *see also* ANDERSON: *Fitting a Virtual Peg…*, p. 142.
[56] McDONALD and McLEOD: *'Antisocial Behaviour…*, p. 422.
[57] THE WHITE HOUSE. *Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment [online]*. 29 December 2016 [viewed 23 February 2023]. Available from: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and; *See also* HAATAJA, S. *Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics*. 1st ed. Oxfordshire: Routledge, 2020, pp. 180-181.
[58] BBC. US imposes new Russia sanctions over cyber-attacks. *bbc.com* [online]. 11 June 2018 [viewed 23 February 2023]. Available from: https://www.bbc.com/news/world-us-canada-44446449; U.S. DEPARTMENT OF THE TREASURY. Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks. *treasury.com* [online]. 15 March 2018 [viewed 23 February 2023]. Available from: https://home.treasury.gov/news/press-releases/sm0312; HAATAJA: *Cyber Attacks and…*, p. 181.
[59] MORELLO, C. and NAKASHIMA, E. U.S. imposes sanctions on North Korean hackers accused in Sony attack, dozens of other incidents. *washingtonpost.com* [online]. 13 September 2019 [viewed 23 February 2023]. Available from: https://www.washingtonpost.com/national-security/us-sanctions-north-korean-hackers-accused-in-sony-attack-dozens-of-other-incidents/2019/09/13/ac6b0070-d633-11e9-9610-fb56c5522e1c_story.html.

government - Lazarus Group, Bluenoroff, and Andariel.[60] The content of the sanctions is the blocking of the assets of the affected entities and the possible sanctioning of persons which "engage in certain transactions with the entities".[61] Again, these are measures not prohibited under international law, and thus constitute a mere retorsion.[62]

One of the most successful cyber operations (from an attacker's point of view) of recent years was the so-called "SolarWind hack" of 2020. In this operation, Russian intelligence[63] managed to spy on private companies and US government agencies for several months via malicious code.[64] Spying is not an illegal act under international law,[65] and so there could be no other response to this operation than one that does not go beyond retorsion. Thus, in response to this cyber operation, the US banned US banks from trading in certain ruble-based financial products, sanctions also targeted individuals and companies associated with Russian cyber activities, and there were expulsions of several Russian officials from the US.[66]

However, taking action on malign cyber operations is not only a US privilege. In 2020, the European Union adopted its first sanctions related to cyber activities, affecting six individuals and three other entities. These sanctions included "travel bans", "freezing of assets" and prohibition "to make funds available to those individuals and entities listed".[67] This was implemented in accordance with the "cyber diplomacy toolbox" (see below).

These mechanisms adopted in response to cyber operations are often referred to variously, for example as "measures" or "sanctions". In most cases, however, these are actions that can be subsumed under the concept of retorsion (actions not prohibited by international law but hostile to another state or its nationals). This term is not commonly used by states to classify their actions, and thus can hardly be expected to appear in the media or in lay discussion.[68] Nevertheless, its use

---

[60] U.S. DEPARTMENT OF THE TREASURY: Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups. *treasury.com* [online]. 13 September 2019 [viewed 23 February 2023]. Available from: https://home.treasury.gov/news/press-releases/sm0312.
[61] U.S. DEPARTMENT OF THE TREASURY: *Treasury Sanctions North Korean…*
[62] LOTRIONTE, C. Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law. *The Cyber Defense Review*, 2018, 3(2), p. 92; KOSSEFF: *Retorsion…*, p. 18.
[63] McDONALD and McLEOD: *'Antisocial Behaviour…*, p. 431.
[64] JIBILIAN, I. and CANALES, K. The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal. *businessinsider.com* [online]. 15 April 2021 [viewed 23 February 2023]. Available from: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.
[65] SCHMITT et al: *Tallinn Manual 2.0...* , p. 168.
[66] McDONALD and McLEOD: *'Antisocial Behaviour…*, pp. 422, 431; U. S. DEPARTMENT OF STATE. Holding Russia To Account. *state.gov* [online]. 15 April 2021 [viewed 23 February 2023]. Available from: https://www.state.gov/holding-russia-to-account/.
[67] EUROPEAN UNION EXTERNAL ACTION. EU imposes first ever cyber sanctions to protect itself from cyber-attacks. *eeas.europa.eu* [online]. 30 July 2020 [viewed 23 February 2023]. Available from: https://www.eeas.europa.eu/eeas/eu-imposes-first-ever-cyber-sanctions-protect-itself-cyber-attacks_en.
[68] McDONALD and McLEOD: *'Antisocial Behaviour…*, p. 430.

would be appropriate, at least in professional debate and in communicating the measures taken by the state authorities to the international community. Clearer communication would eliminate ambiguity, reduce the risk of escalation, and signal to the state concerned the legal basis on which the state is basing its chosen course of action (in the case of retorsion, the absence of a legal prohibition against such action rather than the existence of explicit permission).

It is clear from the examples given that states use measures falling under the concept of retorsion in response to cyber operations. They just do not use this label for them. However, practice seems to be changing, as the term retorsion has started to appear in official documents related to the application of international law in cyberspace since 2019. The next section of the paper is devoted to these official positions.

1.3.2 Public statements

The first formal statement on the use of retorsion in response to a malign cyber operation can be attributed to the US. Brian J. Egan, Legal Advisor of the US Department of State, in a speech at Berkeley Law School in 2016, stated, "...a state can always undertake unfriendly acts that are not inconsistent with any of its international obligations in order to influence the behavior of other states. Such acts - which are known as acts of retorsion - may include, for example, the imposition of sanctions or the declaration that a diplomat is *persona non grata*."[69] Other states have subsequently taken a similar view in their national positions, namely the Netherlands (2019),[70] New Zealand

[69] EGAN, B. J. International Law and Stability in Cyberspace. *justsecurity.org* [online]. 10 November 2016 [viewed 23 February 2023]. Available from: https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf; UNITED NATIONS. Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266 of 13 July 2021, UN Doc. A/76/136 [online] p. 30. [viewed 24 February 2023] Available from: https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf.

[70] GOVERNMENT OF THE KINGDOM OF THE NETHERLANDS. *Appendix: International law in cyberspace*. [online]. Available from: https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf.

(2020),[71] Estonia (2021),[72] Germany (2021),[73] Norway (2021),[74] Singapore (2021),[75] Switzerland (2021)[76] and the United Kingdom (2022).[77]

There is nothing to be learned from these national positions that would change the view of the concept of retorsion as presented in the first part of the paper, and therefore there is no reason to discuss the individual national positions. The crucial point is that the use of this concept is gaining more and more support in state practice and we can expect this trend to continue in the future.

However, it is worth noting the specific actions that states cite as examples of measures that fall under the concept of retorsion. These include expulsion of diplomats,[78] asset freezes,[79] travel bans,[80] economic or other measures against individuals and entities,[81] "limiting or cutting off the other state's access to servers or other digital infrastructure in its territory",[82] limiting or breaking off diplomatic relations,[83] imposing sanctions,[84] publicly attributing a cyber operation to another state,[85] refraining from signing a trade agreement,[86] recalling an ambassador,[87] restrictions on freedom of movement[88] and exclusion from international groupings.[89]

---

[71] DEPARTMENT OF THE PRIME MINISTER AND CABINET, NEW ZEALAND. *The Application of International Law to State Activity in Cyberspace*. [online]. Available from: https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf.
[72] UN *Official compendium of voluntary national contributions...,* pp. 23-30.
[73] THE FEDERAL GOVERNMENT OF GERMANY. *On the Application of International Law in Cyberspace*. [online]. Available from: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.
[74] UN *Official compendium of voluntary national contributions...,* pp. 65-75.
[75] UN *Official compendium of voluntary national contributions...,* pp. 83-85.
[76] FEDERAL DEPARTMENT OF FOREIGN AFFAIRS OF SWITZERLAND. *Switzerland's position paper on the application of international law in cyberspace*. [online]. Available from: https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf.
[77] FOREIGN, COMMONWEALTH AND DEVELOPMENT OFFICE OF THE UNITED KINGDOM. *Application of international law to states' conduct in cyberspace: UK statement.* [online] Available from: https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.
[78] UN *Official compendium of voluntary national contributions...,* p. 29.
[79] Ibid.
[80] Ibid.
[81] GOVERNMENT OF THE KINGDOM OF THE NETHERLANDS. *Appendix: International law…*
[82] Ibid.
[83] UN *Official compendium of voluntary national contributions...,* p. 72.
[84] Ibid.
[85] UN *Official compendium of voluntary national contributions...,* p. 72.
[86] FEDERAL DEPARTMENT OF FOREIGN AFFAIRS OF SWITZERLAND. *Switzerland's position paper…*
[87] Ibid.
[88] BRAVERMAN, S. International Law in Future Frontiers: The Attorney General, the Rt Hon Suella Braverman QC MP, this evening set out in more detail the UK's position on applying international law to cyberspace. *gov.uk* [online]. 19 May 2022 [viewed 24 February 2023]. Available from: https://www.gov.uk/government/speeches/international-law-in-future-frontiers.
[89] Ibid.

The importance of collective actions based on retorsion, which naturally achieve greater effectiveness, is also emphasized.[90] This is, after all, one of the basic principles also mentioned in the "cyber diplomacy toolbox" of the European Union.[91]

1.3.3 European Union Cyber Toolbox

Cybersecurity is one of the priorities of the European Union (EU). The EU is facing a high number of malign cyber operations and is therefore striving for a secure internet enshrined in international law.[92] To this end, it adopted in 2017 the so-called "cyber diplomacy toolbox", or Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities.[93] This document set out the basic principles for taking defensive measures in the event that the EU or a Member State falls victim to a cyber operation. Among other things, it states that the response to a cyber operation must "be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity" and must also "respect applicable international law and must not violate fundamental rights and freedoms".[94] The toolbox broadly encompasses "diplomatic measures" that can be taken in response to a malign cyber operation in order to influence the actions of the aggressor and achieve redress while avoiding the risk of escalation.[95] Its disclosure then also pursues the preventive goal of deterring a potential aggressor.[96] From the perspective of international law, these are primarily measures falling under the concept of retorsion, but they are also partly countermeasures and plea of necessity, and in the case of the most serious cyber operations amounting to an armed attack, the right of self-defence under Article 51 of the UN Charter also comes into play.[97]

---

[90] BRAVERMAN: *International Law in Future Frontiers…*; UN *Official compendium of voluntary national contributions...,* p. 28.
[91] EUROPEAN PARLIAMENTARY RESEARCH SERVICE: *Understanding the EU's Approach…,* p. 9.
[92] Ibid., p. 1.
[93] COUNCIL OF THE EUROPEAN UNION. Council Conclusions On A Framework For A Joint EU Diplomatic Response To Malicious Cyber Activities ("Cyber Diplomacy Toolbox") of 19 June 2017. Available from: https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf.
[94] Ibid, p. 4
[95] THE NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE. European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox. *ccdcoe.org* [online]. [viewed 23 February 2023]. Available from: https://ccdcoe.org/incyder-articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/; EUROPEAN PARLIAMENTARY RESEARCH SERVICE: *Understanding the EU's Approach…,* p. 2; *see also* MORET, E. and PAWLAK, P. The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime? *iss.europa.eu* [online]. 12 July 2017 [viewed 23 February 2023], p. 2. Available from: https://www.iss.europa.eu/content/eu-cyber-diplomacy-toolbox-towards-cyber-sanctions-regime.
[96] EUROPEAN PARLIAMENTARY RESEARCH SERVICE: *Understanding the EU's Approach…,* p. 8.
[97] EUROPEAN PARLIAMENTARY RESEARCH SERVICE: *Understanding the EU's Approach…,* p. 2; COUNCIL OF THE EUROPEAN UNION. Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities of 9 October 2017, p. 10. Available from: https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf.

The cyber diplomacy toolbox is developed by two further related documents, Council Decision 2019/797 of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States and Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.[98] Both of these documents provide a similar definition of the term "cyber-attack" and define more detailed conditions of freezing of funds and economic resources, i.e. one of the common forms of retorsion (Article 3 of the Regulation and Article 5 of the Decision).

The implementation guidelines for the cyber diplomacy toolbox set out a category of restrictive measures which may by imposed "against third countries, entitities or individuals".[99] These measures may include, inter alia, "travel bans, arms embargoes, freezing funds or economic resources".[100] The guidelines also explicitly mention that measures adopted under the cyber diplomacy toolbox may also be used to support individual and collective measures taken by Member States in accordance with international law.[101] Other official EU documents even refer to collective action as necessary "for the response to be effective".[102] Without specifying what the measures are, the reference to international law makes it clear that the guidelines target countermeasures, plea of necessity and the right of self-defence. Given the impossibility of assistance in the case of countermeasures (third-party countermeasures are not allowed), then this assistance, at least in this case, must consist precisely of retorsion.

The EU has therefore defined a range of measures, from retorsion to self-defence. All of these concepts can be used, but always with full respect for the requirements of international law for each instrument. When examples of specific measures are mentioned in official documents, they generally fall under the concept of retorsion. Unsurprisingly, cooperation between Member States is crucial for the EU, which is also reflected in the requirement for other Member States to support the measures taken.

---

[98] COUNCIL OF THE EUROPEAN UNION. Council Decision 2019/797 of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States; Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.
[99] COUNCIL OF THE EUROPEAN UNION. *Draft implementing guidelines…,* p. 9.
[100] COUNCIL OF THE EUROPEAN UNION. *Draft implementing guidelines…,* p. 9.
[101] Ibid.
[102] EUROPEAN PARLIAMENTARY RESEARCH SERVICE: *Understanding the EU's Approach…,* p. 8.

1.4 Available retorsion measures

Retorsion is not a new concept that is unique to responses to cyber operations.[103] It is merely experiencing a renaissance of its own and finding new meaning in the context of the opaque environment of cyberspace, where the intensity of violations of international law can be negligible or extreme, and where the attribution of actions to a particular state is a fundamental problem. The development of technology has given rise to new threats that need to be defended against, while at the same time creating space for the implementation of new retaliatory measures. These can be divided into traditional measures, unrelated to cyberspace, and modern measures, implemented in or through cyberspace (cyber retorsion). The following part of the paper is divided according to this key.

1.4.1 Non-cyber related measures (traditional retorsion)

As a rule, traditional measures that can be described as retorsion are not problematic from the perspective of international law.[104] As the literature and state practice (see above) show, there is a relatively settled repertoire of measures. These are mainly:

- official statements (e.g. protests),
- denial of access to state resources,
- expulsion of diplomats,
- economic sanctions,
- travel bans,
- freezing of assets,
- arms embargoes,
- limiting or breaking off diplomatic relations,
- refraining from signing a trade agreement,
- ending participation in a treaty,[105]
- withdrawing from an international organization,[106]
- recalling own ambassador,

---

[103] McDONALD and McLEOD: *'Antisocial Behaviour…*, p. 443.
[104] ROGUSKI, P. *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*. The Hague Program For Cyber Norms Policy Brief. 2020, p. 18. Available from: https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/153989/roguski_application_of_international_law_to_cyber_operations_2020.pdf?sequence=1&isAllowed=y.
[105] McDONALD and McLEOD: *'Antisocial Behaviour…*, p. 427.
[106] Ibid.

- summoning a foreign ambassador,[107]
- restriction of movement,
- exclusion from international groupings,
- canceling bilateral visits,[108]
- denying access to ports,[109]
- boycott of the Olympic Games,[110]
- renaming of a place (e.g. street, square),[111]
- terminating cultural and educational exchanges,[112] and
- reduction of foreign aid.[113]

A specific type of retorsion related to cyber operations, which is not itself implemented through cyberspace but usually takes the form of an official statement, is the attribution of a cyber operation to a responsible state.[114] Norway has also explicitly subsumed this practice under retorsion in its official national position.[115] The aim of this attribution is the so-called "public shaming" of a responsible state, which affects its international reputation and creates pressure to respect international law and refrain from similar (sanctioned) actions in the future. An example of this is the designation of the Russian government as the originator of the NotPetya malware in 2018 by a broad coalition of states including, among others, the US, the UK, Estonia and Denmark.[116] Domestic indictment of entities and individuals from responsible state can play a similar role.[117] In the context of public attribution of a conduct to a state, technical information may also be disclosed to enable more effective defense against similar cyber operations by other states, which in itself may constitute a type of retorsion.[118]

It should be noted that in implementing retorsion measures, it is always necessary to take into account the possible treaty obligations of the states involved, which may give rise to rights and

---

[107] McDONALD and McLEOD: *'Antisocial Behaviour…,* p. 427.
[108] Ibid.
[109] Ibid.
[110] Ibid.
[111] DAWIDOWICZ: *Third-Party Countermeasures…,* p. 28; For example, Prague renamed the street where the Russian Embassy in the Czech Republic is located to "Ukrajinský hrdinů" (Ukrainian Heroes) in reaction to the Russian-Ukrainian war of 2022, *see* Dohnalová, A. and Bartoníček, R. Ukrajinských hrdinů. Praha přejmenovala část ulice Korunovační u ruské ambasády. *aktualne.cz* [online]. 22 April 2022 [viewed 23 February 2023]. Available from: https://zpravy.aktualne.cz/regiony/praha/ukrajinskych-hrdinu-praha/r~92302b02c21411ec8a24ac1f6b220ee8/.
[112] LOTRIONTE: *Reconsidering the Consequences…*, p. 92.
[113] ARSIWA, p. 128.
[114] McDONALD and McLEOD: *'Antisocial Behaviour…,* p. 431.
[115] UN *Official compendium of voluntary national contributions...*, p. 72.
[116] Ibid.
[117] KOSSEFF: *Retorsion…*, p. 17.
[118] THE WHITE HOUSE. *Fact Sheet: Actions in Response…*; HAATAJA: *Cyber Attacks and…,* pp. 180-181.

obligations not provided for by general international law.[119] Treaties are a source of international law and may limit the retorsion measures available in a particular situation. Therefore, it cannot be stated in general terms that the above list of traditional measures is always and universally available to all states; on the contrary, each case must be considered on its own merits.[120]

This conflict with treaty obligations often arises particularly in relation to economic sanctions, as international economic relations and trade are subject to considerable international legal regulation (e.g. World Trade Organization). Despite the fact that even the International Court of Justice in the Nicaragua case pronounced that economic measures consisting of the termination of economic aid, a significant reduction of the sugar quota and trade embargo are not contrary to international law,[121] special attention should be paid to these measures, not only from the perspective of treaty obligations, but also in relation to a possible violation of the principle of non-intervention.[122]

1.4.2 Cyber related measures (cyber retorsion)

The shift of part of interstate interaction to cyberspace has also given rise to new types of retorsion. These are actions that are directly related to cyberspace (performed in or through it) and meet the defining characteristics of retorsion (unfriendly, but lawful). A thorough analysis of this topic is provided by Jeff Kosseff in his 2020 article.[123]

Limitation of access to cyber infrastructure

States have full sovereignty over the cyber infrastructure located on their territory.[124] It is therefore entirely at the discretion of the state as to whom and how it allows this infrastructure to be used, just as it decides on the use of its own territory. Thus, one typical measure that is not contrary to international law is restricting another state's access to national infrastructure.[125] The only limit to this is any treaty obligations relating to cyber infrastructure.[126] Restriction of access was already implemented in practice by Estonia in 2007 when it banned access to certain IP addresses registered

---

119 RUYS: *Sanctions, Retorsions…*, p. 24; SCHMITT et al: *Tallinn Manual 2.0...* , p. 112.
120 SCHMIDT: *The Legality of…*, p. 71.
121 *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, ICJ, Judgement, 27 June 1986, para. 244-245 (hereinafter "Nicaragua v. United States").
122 For a thorough discussion of the issue, see RUYS: *Sanctions, Retorsions…*, p. 24; *see also* SCHMIDT: *The Legality of…*, p. 71.
123 KOSSEFF: *Retorsion…,* pp. 17-22.
124 SCHMITT et al: *Tallinn Manual 2.0...* , p. 13.
125 Ibid, p. 112.
126 LOTRIONTE: *Reconsidering the Consequences…*, p. 92.

in Russia.[127] Such a practice is also considered a legitimate retorsion by the Netherlands, which mentions "limiting or cutting off ... access to servers or other digital infrastructure" in its official position on the application of international law in cyberspace.[128]

Gathering information

Gathering information may take place on state's own cyber infrastructure or on the adversary's infrastructure.

Monitoring and documenting an attacker's activities on state's own networks does not raise any international law issues.[129] It is the activity of the victim state on its territory and in its cyber infrastructure, which is fully covered by the principle of territorial sovereignty. The information gathered in this way can fulfil several roles in the later phase. It can be used to improve state's own cybersecurity, it can be provided (publicly or non-publicly) to partners and, of course, it can also be used as evidence to prove the accountability of the responsible state.

Honeypots are a specific technique of gathering information about adversary activities on the target state's cyber infrastructure. It is defined as follows: "A deception technique in which a person seeking to defend computer systems against malicious cyber operations uses a physical or virtual environment designed to lure the attention of intruders with the aim of: deceiving the intruders about the nature of the environment; having the intruders waste resources on the decoy environment; and gathering counter-intelligence about the intruder's intent, identity, and means and methods of cyber operation."[130] In other words, the target state creates a cyber infrastructure that outwardly gives the appearance of being a relevant target for a cyber operation (e.g., military or government servers), but in reality is a false infrastructure containing no relevant information. On the contrary, such an infrastructure is equipped with software through which the activities of the attacker in this "fake infrastructure" are monitored in detail. The use of this technique in its basic form meets the definition of retorsion. However, this may not be the case for so-called "weaponized honeypots" (see below).

The collection of information about the aggressor and its activities can also occur directly in its cyber infrastructure. Then we need to talk about "cyber espionage".[131] Espionage is generally not

---

[127] SCHMITT et al: *Tallinn Manual on the International Law Applicable to Cyber Warfare…*, p. 40.
[128] GOVERNMENT OF THE KINGDOM OF THE NETHERLANDS. *Appendix: International law…*
[129] KOSSEFF: *Retorsion…*, p. 19.
[130] SCHMITT et al: *Tallinn Manual 2.0...* , p. 565.
[131] KOSSEFF: *Retorsion…*, p. 18.

prohibited by international law and is therefore nothing more than retorsion.[132] However, only the acquisition of information without simultaneously altering, damaging or removing the data in question can be considered espionage, since otherwise it would constitute at least an interference with the sovereignty of the state concerned.[133]

Operations on or against adversary's cyber infrastructure

Merely mapping an adversary's cyber infrastructure without manipulating the data is a form of espionage and as such constitutes a retorsion in terms of international law. However, if, in the context of such a cyber operation, interference is made with that infrastructure, e.g. for the purpose of "preparation of battlefield" in order to make possible future retaliation more effective, such an operation may be considered an interference with the sovereignty of the state concerned, and therefore is not a retorsion and needs to be justified by another instrument of international law (e.g. countermeasures).[134]

The use of weaponized honeypots is a separate category of cyber operations with consequences in the cyber infrastructure of an adversary, which is a subject of expert debate.[135] Honeypots in this case do not only contain meaningless data, but in addition, malicious code (malware) is also hidden in this data, which the attacker, through his own activity, transfers to his own network, where this code can "cause significant disruption or damage in the target system".[136] The crucial question is whether, in this context, where the transmission of the malicious code was carried out by the injured state of its own will (state B), the international legal liability of the state that set the trap (state A) can be inferred. Although most experts involved in the drafting of the Tallinn Manual 2.0 are inclined to conclude that state A's responsibility cannot be inferred (only state B acted actively),[137] there are compelling arguments to the contrary. First of all, the exfiltration of data from state A's network is nothing but espionage, i.e. lawful conduct. Again, only lawful conduct, i.e., retorsion, comes into play in response to such conduct. Malicious code that causes damage on the part of state B would, if actively carried out by state A, undoubtedly be an internationally wrongful act. By setting a trap with malicious code, state A makes it clear that it is at least aware that the

---

[132] SCHMITT et al: *Tallinn Manual 2.0...* , p. 168.
[133] SCHMITT et al: *Tallinn Manual 2.0...* , p. 168.; KOSSEFF: *Retorsion…,* p. 19.
[134] KOSSEFF, J. *Retorsion…,* pp. 21-22; CHESNEY, R. The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes. *lawfareblog.com* [online]. 25 September 2018 [viewed 19 February 2023]. Available from: https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes.
[135] KOSSEFF: *Retorsion…,* p. 20.
[136] SCHMITT et al: *Tallinn Manual 2.0...* , p. 174.
[137] Ibid.

code will be transmitted by another state to its network and cause damage. Thus, applying the concept of culpability from criminal law by analogy, it is indirect intent (*dolus eventualis*) that gives rise to criminal liability of the perpetrator in national criminal codes.[138] There is no reason why this should be otherwise at the level of international law. It can therefore be concluded that weaponized honeypots do not fall into the category of retorsion and that the fulfilment of the prerequisites of one of the circumstances precluding wrongfulness is required to justify them.[139]

However, this conclusion only applies to malware that manipulates data (modification, deletion, making it inaccessible, etc.). If the exfiltrated malware is intended only to map the adversary's network and transfer data "home", it is permissive cyber espionage without international legal consequences.[140]

Kosseff also includes operations aimed at "slowing down the adversary" under retorsion, citing as an example Operation Glowing Symphony against ISIS, during which US Cyber Command removed data and restricted access to ISIS media systems.[141] In his view "[s]uch slow-down operations are unfriendly, but absent more significant harms there is at least a reasonable argument that the operations are retaliatory". It is not possible to agree with this conclusion. As noted above, cyber espionage is considered lawful. However, the moment data is interfered with (tampered with, removed), it is undoubtedly at least an interference with the sovereignty of another state (and potentially a more serious violation of international law).[142] Such an interference does not meet the defining characteristics of retorsion and requires justification by another instrument of international law for its legality.

Warning of individual operatives

In some cases, states are able to identify the specific individuals conducting cyber operations.[143] It may then be possible to establish direct communication with these individuals. The US used this approach when it contacted Russian operatives behind the spread of disinformation in connection with the electoral processes and sent them a message informing them that "American operatives

---

[138] *See* SPÁČIL, J. Animus Aggressionis: The Role Of Intent in the Analysis of Armed Attack in Cyberspace. *Czech Yearbook of Public & Private International Law*, 2022, 13(1), pp. 58-59.
[139] WALLACE, D. and VISGER, M. The Use of Weaponized "Honeypots" under the Customary International Law of State Responsibility. *Cyber Defense Review*, 2018, 3(2), p. 38.
[140] Ibid, p. 33
[141] KOSSEFF: *Retorsion…,* p. 22.
[142] SCHMITT et al: *Tallinn Manual 2.0...* , p. 19.
[143] KOSSEFF: *Retorsion…,* p. 17.

have identified them and are tracking their work".[144] Although the content of the message was not a direct threat, any operative so contacted could infer that "[he or she] could be indicted or targeted with sanctions". [145]

The conclusion as to whether the above practice can be considered as retorsion depends on the content of the specific communication. A mere communication on the basis of "we know who you are and what you do" does not constitute a violation of international law and is retorsion. However, if there is for example a direct threat to physically eliminate a person, it could already be an unlawful violation of the prohibition on the threat of the use of force or another rule of international law.[146]

1.5 Conclusion

The aim of this paper was to define the role of retorsion (unfriendly, but lawful conduct) in defence against malign cyber operations and to determine which measures can be subsumed under this concept.

In the first part of the paper, the concept of retorsion and its position from the perspective of international law was explained, as it is an area that has not received sufficient attention from international legal scholarship (which has been changing in recent years). It was clarified that retorsion is more of a technical and descriptive term rather than legal instrument.

In the second part of the article, attention was paid to state practice. Using concrete examples of state conduct and referring to official documents of a number of states, it was shown that retorsion is slowly but surely returning to the international lexicon and that the trend can be expected to continue.

The third part was devoted to specific measures that meet the definition of retorsion. These measures have been divided into two categories, namely "traditional retorsion" and "cyber retorsion". While the first category includes measures that have been used since time immemorial, the second category includes measures specific to cyber operations that have only developed in recent years. These include measures related to restricting access to one's own cyber infrastructure, information gathering and cyber espionage, operations on or against adversary's cyber infrastructure and warning of individual operatives.

---

[144] BARNES, E. J. U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections. *nytimes.com* [online]. 23 October 2018 [viewed 23 February 2023]. Available from: https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html.
[145] Ibid.
[146] KOSSEFF: *Retorsion…*, p. 21.

In conclusion, it should be noted that retorsion is an important concept in international law that allows states to respond to all types of cyber operations, regardless of their severity, legality, or originator. Although these are rather less effective measures, they certainly have their place in the repertoire of retaliatory measures, as recent state practice demonstrates. In the future, we can expect more frequent use of this term to describe measures taken in response to cyber operations. In terms of further research, particular attention will need to be paid to the limits of retaliatory measures implemented directly on another state's cyber infrastructure, as there is a certain grey area and undeniable tension between retorsion and interference with that state's sovereignty.

2 Plea of Necessity: A legal key to protection against unattributable cyber operations[147]

2.1 Introduction

The development of information technology has been a source of unprecedented economic growth for companies and an increase in the standard of living for individuals. At the same time, however, it also brings risks. Modern societies and their survival literally depend on computer-controlled systems (water distribution, healthcare system, electricity distribution, to mention just a few). It is therefore not surprising that cybersecurity is becoming a topic of paramount importance.

States are increasingly forced to confront cyber operations that result in economic and material damage.[148] In the case of a domestic cyber operation, states generally have sufficient domestic legal means to protect themselves (for example, through police or military action). However, a problem arises when the cyber operation originates in the territory of another state. In this situation, international law and its fundamental principles, such as sovereignty, the prohibition of interference or the prohibition of the use and threat of force, come into play, which significantly limit the legal ability of the victim state to defend itself against a cyber operation from another state. The victim state is thus forced to choose between retorsion, countermeasures, self-defense, and plea of necessity, each of which is limited by a number of conditions and varies in effectiveness.

A fundamental issue that influences considerations on the choice of an appropriate defensive measure is the question of the attributability of a cyber operation to the state from whose territory it is carried out. A distinction must be made between attribution in the legal and technical sense. Attributability of acts in the legal sense, although not free from some controversies, has already been clarified to a large extent in the work on the Draft Articles on Responsibility of states for Internationally Wrongful Acts ("ARSIWA") carried out by the International Law Commission and in the jurisprudence of international tribunals.[149] However, attribution in the technical sense is particularly problematic, because while in the case of a conventional attack it is relatively easy to

---

[147] This work was originally published in the Masaryk University Journal of Law and Technology [SPÁČIL, J. Plea of Necessity: Legal Key to Protection against Unattributable Cyber Operations. *Masaryk University Journal of Law and Technology*, 2022, 16(2), pp. 215 - 239] and won the first place in the faculty round of the competition in Student Scientific and Professional Activities (SVOČ 2022) and third place in the Czech-Slovak final. Research was supported by the student project "Action in plea of necessity as a defence against cyber operations of non-state actors" of the Palacký University in Olomouc. The work was prepared under the supervision of prof. JUDr. Dalibor Jílek, CSc.

[148] In 2021 alone, 118 cyber incidents were recorded and classified as "significant" by the Center for Strategic & International Studies, including a ransomware attack on the Colonial Pipeline, "the largest fuel pipeline in the United States"; CENTER FOR STRATEGIC & INTERNATIONAL STUDIES. *Significant cyber incidents*. [online] Washington, D. C.: CSIS [viewed 3 January 2022]. Available from: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[149] ARSIWA, art. 4 - 11; Nicaragua v. United States, paras. 105-115.

determine the place of origin of the threat (e.g. the place of launch of a missile, the place of launch of bombers) using modern military technology, and the very nature of the weapon used will tell us something about the origin of the operation, in cyberspace the situation is much more complex. The means to carry out a cyber operation are freely available to almost anyone, just a few mouse clicks away. If it is a sophisticated cyber operation, then it usually involves masking the origin, for example by redirecting traffic through third countries. And even if the specific device from which the cyber operation was carried out can be identified, the search for the perpetrator is not over, as it may be difficult to determine who controlled the device and whether the link between that person and the state existed or was sufficiently intense to meet the requirements for legal attribution of the conduct to the state.

Thus, in the case of cyber operations, it is very often impossible to prove that they are attributable to another state. In such circumstances, the attacked state finds itself in a difficult situation, since attribution of the operation to a state is an element of internationally wrongful act which itself is one of condicions *sin qua non* for applicability of most of the circumstances precluding wrongfulness under international law. One of the few such circumstances that are applicable even in the absence of attribution (and internationally wrongful act) is the plea of necessity.[150] This is the reason why this instrument has received increasing attention in recent years, not only in the scholarly debate,[151] but references to this instrument are also beginning to appear in the national cyber strategies of a number of states.[152]

The aim of this paper is a detailed analysis of the plea of necessity and its applicability in the context of cyber operations. As the plea of necessity is not an instrument of international law that is free from controversy, the paper also examines the problematic aspects of this instrument, in particular the possibility of the use of force.

The paper is divided into two main parts. The first part is devoted to the explanation of the concept of plea of necessity and its comparison with retorsion, countermeasures and self-defence and to the definition of their mutual advantages and disadvantages. The second part of the paper explains

---

150 SCHMITT, M. N. Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum. *Harvard National Security Journal*, 2017, 8 (2), p. 251.

151 A comprehensive analysis of the plea of necessity in the context of cyber operations (with a focus on the use of force) is offered by LAHMANN, H. *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution*. 1st ed. Cambridge: Cambridge University Press, 2020, pp. 201-257; *see also* ARIMATSU, L. and SCHMITT, M., N. The Plea of Necessity: An Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 2021, 97(1), pp. 1171-1198.

152 Six states have so far explicitly expressed their support for the plea of necessity in the context of cyber operations: the Netherlands (2019), France (2019), Germany (2021), Japan (2021), Norway (2021) and Switzerland (2021). An overview of their positions is available from: https://cyberlaw.ccdcoe.org/wiki/Plea_of_necessity [viewed 3 January 2022].

and discusses the various conditions and limits of the application of plea of necessity, including its problematic aspects.

2.2 Plea of necessity and other circumstances precluding wrongfulness

Necessity is one of the instruments of international law that allows a state acting under it to temporarily disregard its obligations under international law when necessary to protect the "essential interest" of that state.[153] The plea of necessity therefore appears to be an appropriate legal basis, for example, in a situation where a state is the victim of a cyber operation originating in the territory of another state, but it cannot be shown that the state is responsible (it is attributable to it) nor has it breached the obligation of due diligence, since the application of the plea of necessity is not premised on an internationally wrongful act of another state.[154] It is this aspect that makes the plea of necessity a suitable instrument to justify a protective measure against a cyber operation of unknown origin or carried out by a non-state actor from the territory of another state.[155]

Plea of necessity is a "circumstance precluding wrongfulness" of an act, the definition of which can be found in Article 25 of ARSIWA. The definition reads:[156]

Necessity may not be invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of that State unless the act: (a) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and (b) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole.
2. In any case, necessity may not be invoked by a State as a ground for precluding wrongfulness if: (a) the international obligation in question excludes the possibility of invoking necessity; or (b) the State has contributed to the situation of necessity.

It follows from this definition that the plea of necessity is available to the state only under strict conditions aimed at limiting the possibility of abuse of this instrument.[157] It is an instrument which "can only be accepted on an exceptional basis"[158] and whose threshold is extremely high.[159] The exceptional nature of the plea of necessity is also confirmed by the negative wording of this article

---

153 ARSIWA, art. 25 (1) (a).
154 ARSIWA, art. 25, p. 80, para. 2.
155 ARIMATSU and SCHMITT: *The Plea of Necessity…*, p. 1185-1186.
156 ARSIWA, art. 25.
157 ARSIWA, art. 25, p. 80, para. 2.
158 *Case Concerning The Gabčíkovo-Nagymaros Project (Hungary v. Slovakia)*, ICJ, Judgement, 25 September 1997, para. 51 (hereinafter "Gabčíkovo-Nagymaros").
SCHMITT et al: *Tallinn Manual 2.0...*, p. 135.

of ARSIWA.[160] The International Court of Justice (hereinafter "ICJ") in the Gabcikovo-Nagymaros judgment stated the customary character of this instrument and explicitly mentioned certain conditions of the plea when it stated that in relation to the act to be plea of necessity justified, "it must have been occasioned by an 'essential interest' of the state which is the author of the act conflicting with one of its international obligations; that interest must be threatened by a 'grave and imminent peril'; the act being challenged must have been the 'only means' of safeguarding that interest; that act must not have 'seriously impair[ed] an essential interest' of the state towards which the obligation existed; and the state which is the author of that act must not have 'contributed to the occurrence of the state of necessity'".[161]

The plea of necessity, given its potential importance, did not escape the attention of the experts drafting the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (hereinafter "Tallinn Experts"), which devoted a separate rule 26 (Necessity) to the plea of necessity: "A state may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding it."[162] Although the restatement of the rule in the Tallinn Manual is considerably more concise than in Article 25 of ARSIWA and does not contain all the conditions listed in Article 25 of ARSIWA, taking into account the commentary to rule 26 of the Tallinn Manual, it must be stated that the conditions within the scope of Article 25 of ARSIWA also form an integral part of this rule under the Tallinn Manual and "there is no substantial discrepancy" between these rules.[163]

A more detailed definition of the terms of plea of necessity in the context of cyber operations will be discussed in the next part of this paper, but first it is necessary to define the differences between plea of necessity and retorsion, countermeasures and self-defence as possible alternatives to justify defensive action against a cyber operation.

The first, the least invasive, and arguably the least effective method of defence, is retorsion. Retorsion is defined as "retaliation for discourteous, or unkind, or unfair and inequitable acts by acts of the same or a similar kind".[164] It is therefore an act, which is unfriendly, but lawful. An example of the use of retorsion in response to a cyber operation is the European Union's action in 2020, when the EU imposed a travel bans and froze the assets of six individuals and three

---

[160] ARSIWA, art. 25, p. 83, para. 14.
[161] Gabcikovo-Nagymaros, para. 51.
[162] SCHMITT: *Peacetime Cyber Responses…*, p. 135.
[163] SCHALLER, C. Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 2017, 95 (1), p. 1624; SCHMITT: *Peacetime Cyber Responses…*, pp. 137-141.
[164] GRANT, BARKER: *Parry & Grant encyclopaedic dictionary…*, pp. 525 - 526.

companies in connection with the Wanna Cry, Not Petya and Cloud Hopper operations.[165] Unlike the plea of necessity, there is no violation of international law requiring justification for the retorsion.

The second option that can be used to defend against a cyber operation are countermeasures. These are such non-forcible measures that an injured state adopts in response to an internationally wrongful act of another state which aim to compel that state to "cessation [of the internationally wrongful act] and to achieve reparation for the injury".[166] Unlike retorsion, which does not constitute a violation of international law, in the case of countermeasures the defending state commits an act which, although objectively fulfilling the elements of a wrongful act, the wrongfulness of the act is excluded precisely because it is a countermeasure within the meaning of Article 22 of ARSIWA. Thus, it is by reference to countermeasures that an interference with the sovereignty of another state can be justified, which gives the victim state the possibility to use a wider range of cyber and other means to defend itself, including defensive cyber operation in the territory of responsible state (hack back).[167] However, invocation of countermeasures is also subject to several conditions. As already noted, countermeasures are only available if there is an internationally wrongful act committed by another state.[168] Thus, a prerequisite for the application of countermeasures is the attributability of the cyber operation to the state.[169] As noted in the introduction to the text, it is the attributability of cyber operations that is highly problematic, and countermeasures will therefore often not be available precisely because the act is not attributable to the state. If the condition of attributability was met, countermeasures would need to be proportional. Proportionality in countermeasures, unlike self-defence, does not refer to the objective pursued (the termination of an internationally wrongful act), but should be assessed as "rough equivalence between the harm caused by the underlying unlawful act and the countermeasure".[170] Proportionality defined in this way severely limits the usefulness of countermeasures, as it significantly restricts the range of available measures. At the same time, countermeasures cannot justify the use of force.[171] Another disadvantage of countermeasures is the fact that their use is not possible against cyber operations launched by non-state actors, unless such

---

165 COUNCIL OF THE EUROPEAN UNION. *EU Imposes the First Ever Sanctions against Cyber-Attacks* [viewed 3 January 2022]. Available from: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/; *see also* ARIMATSU and SCHMITT: *The Plea of Necessity*…, p. 1173.
166 ARSIWA, art. 22, p. 75, para. 1.
167 ARIMATSU and SCHMITT: *The Plea of Necessity*…, p. 1179.
168 ARSIWA, art. 22, p. 75, para. 1; ARSIWA, art. 2: "There is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State."
169 ARSIWA, art. 22, p. 75, para. 1.
170 ARIMATSU and SCHMITT: *The Plea of Necessity*…, p. 1180.
171 ARSIWA, art. 50(1)(a).

conduct is attributable to the state. In order to make the interpretation of countermeasures in the context of cyber operations complete, it should be noted that breach of the due diligence obligation of the territorial state may also may also lead to application of countermeasures. However, the very existence of the due diligence obligation, despite its inclusion in Tallinn Manual 2.0, is controversial.[172]

The third alternative by which a state can respond to the most serious cyber operations that meet the characteristics of an "armed attack" under Article 51 of the UN Charter is self-defence.[173] The right to self-defence is an exception to the prohibition on the use and threat of force.[174] There are three issues associated with the right to self-defence: the possibility of self-defence against non-state actors, attribution and the threshold of an armed attack.

The issue of the use of self-defence against armed attacks carried out by non-state actors is crucial in cyberspace, as proving the relationship between a state and a non-state actor poses significant practical difficulties. However, the answer to the question of whether force can be used against a non-state actor whose actions are not attributable to a state is highly controversial. Prior to the 2001 terrorist attack on the World Trade Center in New York, it was generally accepted that self-defense was only available against armed attacks attributable to a state, even in situations where such an attack was carried out by a non-state actor.[175] In response to the 9/11 attack, however, there has been a shift. In the immediate aftermath, the United Nations Security Council, NATO and individual states viewed this attack, which was not attributable to a specific state, as justifying the use of force in self-defence.[176] However, this approach was later challenged by the ICJ in the Wall Advisory Opinion when it stated that "Article 51 of the Charter thus recognizes the existence of an inherent right of self-defence in the case of armed attack by one state against another state."[177] By its emphasis on "one state against another", the ICJ thus made it clear that the right of self-defence is available only in the case of an armed attack attributable to a particular state. The question of the use of force in self-defense against non-state actors whose conduct is not attributable to a state thus remains a neuralgic point of *jus ad bellum*.

---

[172] SCHMITT: *Peacetime Cyber Responses…*, p. 30.; ARIMATSU and SCHMITT: *The Plea of Necessity…*, p. 1180; SCHALLER: *Beyond Self-Defense and Countermeasures…*, p. 1620.
[173] SCHALLER: *Beyond Self-Defense and Countermeasures…*, p. 1619.
[174] Charter of the United Nations from 1945, Article 2 (4).
[175] Nicaragua v. United States, para. 195.
[176] ARIMATSU and SCHMITT: *The Plea of Necessity…*, p. 1177; *see also* United Nations Security Council, Resolution 1368 (2001) adopted on 12 September 2001 and United Nations Security Council, Resolution 1373 (2001) adopted on 28 September 2001.
[177] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, ICJ, Advisory Opinion, 9 July 2004, para. 139 (hereinafter "Wall Advisory Opinion").

In relation to the issue of attribution, which has been more comprehensively discussed above, it may be briefly added in the context of the right to self-defence that the problematic issue is not so much the legal attribution itself, which is no different from ordinary conventional attacks, but rather the objective demonstration of the existence of relationship between the cyber operation, the originator of the operation and the state. Thus, it is necessary to prove relationships at two levels. At the first level is the relationship between the cyber operation and its perpetrator, i.e. the actual finding of the originator of the operation (a specific device or person). At the second level, it is then a matter of demonstrating a relationship between the originator of the operation and the state that would satisfy the requirements of legal attribution.

A third problematic aspect of the right to self-defence in the context of cyber operations is the determination of the threshold of an "armed attack". The ICJ has held that it is necessary to distinguish "the most grave forms of the use of force", which constitute an armed attack, from "other less grave forms", thus creating room for the use of force, which does not reach the threshold of an armed attack.[178] It can be concluded that the threshold of an armed attack in the cyber context remains unclear.[179] On the one hand, it is widely accepted that cyber operations resulting in personal injury and material damage (e.g. disabling the control system of a power plant, resulting in serious damage to it) fulfil the elements of an armed attack within the meaning of Article 51 of the UN Charter.[180] On the other hand, there is a large group of cyber operations that do not cause the consequences listed above, but whose consequences can nevertheless be described as 'severe harm and disruption' (e.g. widespread disruption of a state's financial system).[181] Thus, drawing a clear dividing line between cyber operations that meet the characteristics of an armed attack and those that are less serious is not yet possible. A more detailed analysis of the issue of armed attack in the cyber context is beyond the scope of this paper.[182]

We have presented a repertoire of legal instruments that states may have at their disposal in the event that they fall victim to a cyber operation. Measures (especially diplomatic) that do not violate international law can be applied in the context of a retorsion. Countermeasures can only be applied in situations where there is an internationally wrongful act attributable to a particular state, and the measures taken under countermeasures must be proportionate to the harm caused. Self-defence is only available where there is an armed attack, and the classification of a cyber operation as an armed

---

178 Nicaragua v. United States, para. 191.
179 ARIMATSU and SCHMITT: *The Plea of Necessity…*, p. 1175.
180 Ibid. We leave aside the issue of the use of force not reaching the intensity of an armed attack.
181 Ibid.
182 For a detailed analysis of approaches to "armed attack" in cyberspace see VALUCH, J and HAMUĽÁK, O. Use of Force in Cyberspace. *International and Comparative Law Review*, 2020, 20 (2), pp. 174-191.

attack is controversial and unclear. At the same time, it is questionable whether action in self-defence can be taken against non-state actors whose actions are not attributable to the state. Alongside these legal instruments stands the plea of necessity.

Plea of necessity has several advantages over the above options. In the first place, the plea of necessity (subject to all the conditions that will be discussed in the next section) justifies the violation of international law and thus allows, for example, a "hack back" operation to violate the sovereignty of another state. The fundamental advantage, then, is that the plea of necessity is available even if the cyber operation against which the victim state is defending itself is not attributable to another state, and it is thus available against non-state actors as well, distinguishing necessity from countermeasures and self-defense. In other words, a plea of necessity can justify measures against a non-responsible state.[183] Plea of necessity can justify even "bleed-over effects" into third states.[184] Finally, unlike countermeasures, plea of necessity is available when harm is imminent, i.e. has not manifested yet.[185] Thus, it is clear that in the context of cyber operations, where the actions of non-state actors are widespread and attribution is often not possible, the plea of necessity is an instrument that can be very attractive for states threatened by cyber operations, since, as Germany has also expressed in its official position on the application of international law in cyberspace, it is available "even in certain situations in which the prerequisites for countermeasures or self-defence are not met".[186] However, the plea of necessity is also inherently associated with a high risk of abuse, and therefore this legal instrument is limited by a number of conditions, to analysis of which is devoted the next section of this paper.

2.3 Preconditions and limitations of plea of necessity

The main objective of international law is "to maintain peace and security through a rules-based system"[187] and the creation of the United Nations was motivated primarily by the objective "to maintain international peace and security".[188] The plea of necessity, while it can be a very effective tool in countering cyber operations, also carries the risk of abuse and escalation, and thus inherently threatens these goals of the international community.[189] It is therefore logical and correct that it is an exceptional measure with a high threshold and that the use of this instrument is limited by a

[183] SCHMITT: *Peacetime Cyber Responses…*, p. 137.
[184] Ibid.
[185] LOTRIONTE: *Reconsidering the Consequences…*, p. 96.
[186] THE FEDERAL GOVERNMENT OF GERMANY. *On the Application of International Law in…,* pp. 14 - 15.
[187] ARIMATSU and SCHMITT: *The Plea of Necessity…*, p. 1173.
[188] Charter of the United Nations from 1945, Article 1 (1).
[189] ARSIWA, art. 25, p. 80, para. 2; SCHALLER: *Beyond Self-Defense and Countermeasures…*, p. 1619.

number of strict conditions that must be insisted upon. We will therefore now turn to the interpretation of these conditions in the context of cyber operations.

2.3.1 Preconditions and limitations under Art. 25 ARSIWA

Essential interest

A state can justify a measure on the basis of plea of necessity only if its "essential interest" is at stake.[190] The ILC Commentary to ARSIWA does not provide a definition of this term, but does provide that "[t]he extent to which a given interest is 'essential' depends on all circumstances, and cannot be prejudged".[191] Essential interest then undoubtedly cannot be limited to "solely a matter of the 'existence' of the state".[192] According to Tallinn Experts, it is true that "the determination of whether an interest is essential is always contextual".[193] A broader range of interests can be included among the essential interests. According to case law, these interests include protection of environment,[194] issues connected to financial obligations,[195] and protection of persons from terrorist attacks.[196] However, this list is by no means exhaustive and reflects only issues that have already been considered before international tribunals. Lotrionte includes among the essential interests "ecological equilibrium, economy, public health, safety, and maintenance of food supply for the population".[197] Schaller points out that essential interests may be interests related to "territorial integrity, political independence, and constitutional order of s state, the maintenance of public security, and the maintenance of the natural environment".[198] If we focus on state practice, we find that Germany includes under the concept of essential interest "certain critical infrastructures" and "protection of its citizens against serious physical harm" and the Netherlands conceives of essential interests more broadly as "services such as the electricity grid, water supply and the banking system".[199] It is thus clear that a wide range of different interests can be subsumed under essential interests and, in essence, this is a relatively flexible condition, the fulfilment of which need not pose a major problem for states. The above positions of Germany and the

---

190 ARSIWA, article 25(1)(a).
191 ARSIWA, art. 25, p. 83, para. 15.
192 INTERNATIONAL LAW COMMISSION. *Yearbook of the International Law Commission: Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, 1980, vol. II, part two, p. 49, para. 32 (hereinafter *"ARSIWA 1980 with commentaries"*).
193 SCHMITT: *Peacetime Cyber Responses…*, p. 135.
194 Gabčíkovo-Nagymaros, para. 53.
195 LAHMANN: *Unilateral Remedies to Cyber Operations…*, p. 208.
196 Lahmann derives the protection of persons from terrorist attacks as an essential interest from the advisory opinion on the Wall. See LAHMANN: *Unilateral Remedies to Cyber Operations…*, p. 208, note 33.
197 LOTRIONTE: *Reconsidering the Consequences…*, p. 97.
198 SCHALLER: *Beyond Self-Defense and Countermeasures…*, p. 1633.
199 THE FEDERAL GOVERNMENT OF GERMANY. *On the Application of International Law in…*; GOVERNMENT OF THE KINGDOM OF THE NETHERLANDS: *Appendix: International law….*

Netherlands imply a considerable overlap between the concept of 'essential interest' and the concept of 'critical infrastructure', so we will look at this relationship in more detail.

The term "critical infrastructure" has no clear definition and different countries classify different technologies and systems under it.[200] However, a refinement of this concept is not necessary to define the relationship between "essential interests" and "critical infrastructure". According to Tallinn Experts, the classification of an infrastructure as critical is "suggestive" but not "determinative" in relation to determining whether it is an essential interest.[201] This means that not all critical infrastructure is essential interest, and at the same time infrastructure that is not designated as critical may be essential interest. The conclusion that not all critical infrastructure is classifiable as essential interest is also supported by the German national position on plea of necessity cited above.[202]

If a cyber operation is carried out against the critical infrastructure of a state, then the decision whether the essential interest of that state has been interfered with has to be "objective and contextual in the sense of reasonableness in the circumstances".[203] Schmitt gives a pertinent example in which the subject of a cyber operation is healthcare cyber infrastructure, and in which he demonstrates the element of contextuality. Schmitt explains that in a case where a cyber operation disrupts a doctor's appointment system, the threshold of the essential interest of a state will not be crossed, but in a situation where a cyber operation "directed at blood banks during a natural disaster with ensuing significant loss of life" occurs, the threshold of essentiality will be crossed.[204] Similarly, a cyber operation aimed at disrupting the distribution of a vaccine against an infectious disease could be assessed. It will make a difference whether it is the distribution of a vaccine against a common seasonal flu or the distribution of a vaccine against covid-19 disease at the height of a pandemic wave during which hospitals are overcrowded. In the former case, the essential interest of a state is unlikely to be affected; in the latter, it probably is.

---

[200] SCHALLER: *Beyond Self-Defense and Countermeasures…*, p. 1632; SCHMITT: *Peacetime Cyber Responses…*, p. 135.
[201] SCHMITT: *Peacetime Cyber Responses…*, p. 135-136.
[202] Use of the phrase "certain critical infrastructure".
[203] ARIMATSU and SCHMITT: *The Plea of Necessity…*, p. 1185; Conversely, LAHMANN: *Unilateral Remedies to Cyber Operations…*, p. 209, does not consider the contextual nature and considers any operation that "partially or entirely disrupts" critical infrastructure as a grave peril.
[204] SCHMITT: *Peacetime Cyber Responses…*, p. 252; For another example of contextual analysis of essential interest *see also* ARIMATSU and SCHMITT: *The Plea of Necessity…*, p. 1184.

Grave and imminent peril

Another prerequisite to acting in plea of necessity is that the essential interest is threatened by "grave and imminent peril".[205] The ILC has stated that "[t]he peril has to be objectively established and not merely apprehended as possible".[206] This idea was elaborated by the ICJ when it stated that peril "has to be duly established at the relevant point in time".[207]

Schaller defines "peril" as "a situation in which harm is likely to occur if no preventive action is taken".[208] While the ILC does not further define gravity, the Tallinn Experts agreed that in order for a "peril" to be considered "grave", such a threat must be particularly serious, disrupting an essential interest "in a fundamental way, such as destroying the interest or rendering it largely dysfunctional".[209] However, the risk of causing material damage or injury is not a prerequisite for grave peril.[210] Germany considers 'large-scale functional impairments' to be grave peril and, according to the Netherlands, the gravity must be assessed 'on a case-by-case basis', while mere 'impediment or inconvenience' cannot be considered grave peril.[211] In terms of severity, the plea of necessity does not require that the threatened consequences reach the level of an armed attack, which is also stated by France in its national strategy.[212] It can be generalized that for the peril to be grave, the potential harm has to be objectively substantial. Following the above example of the attack on healthcare cyber infrastructure, it will certainly not be possible to consider as a grave peril merely making a hospital's website inaccessible to patients (equals to inconvenience), but disconnecting a hospital from its power supply with consequent harm to the health of patients dependent on the medical equipment will qualify as such.

The second qualifying criterion of peril is imminence. The inclusion of this characteristic in Art. 25 ARSIWA implies that the prerequisite for acting in plea of necessity is not the occurrence of damage, but it is possible to act anticipatorily.[213] The ILC has stated that "peril has to be imminent

---

[205] ARSIWA, article 25(1)(a).
[206] ARSIWA, art. 25, p. 83, para. 15; BANNELIER, K. and CHRISTAKIS, T. *Cyber-Attacks: Preventions-Reactions: The Role of States and Private Actors*. 1st ed. Paris: Les Cahiers de la Revue Défense Nationale, 2017, p. 38.
[207] Gabčíkovo-Nagymaros, para. 54.
[208] SCHALLER: *Beyond Self-Defense and Countermeasures*…, p. 1633.
[209] SCHMITT: *Peacetime Cyber Responses*…, p. 136.
[210] SCHMITT: *Peacetime Cyber Responses*…, p. 136; THE FEDERAL GOVERNMENT OF GERMANY: *On the Application of International Law in*…; GOVERNMENT OF THE KINGDOM OF THE NETHERLANDS: *Appendix: International law*…., pp. 7-8.
[211] Ibid.
[212] ARIMATSU and SCHMITT: *The Plea of Necessity*…, p. 1188; THE FEDERAL GOVERNMENT OF GERMANY: *On the Application of International Law in*…; MINISTRY OF DEFENCE OF FRANCE. *International Law Applied to Operations in Cyberspace*. [online] [viewed 5 January 2022], p. 8. Available from: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.
[213] SCHMITT: *Peacetime Cyber Responses*…, p. 251.

in the sence of proximity."[214] However, this does not mean that the imminence of the peril shall be considered only from the point of view of temporary element.[215] To the contrary, the ICJ held that "'peril' appearing in the long term might be held to be 'imminent' as soon as it is established, at the relevant point in time, that the realization of that peril, however far off it might be, is not thereby any less certain and inevitable".[216] At the same time, however, it should be borne in mind that another condition of the plea of necessity is that the action implemented (e.g. hack-back) must be the *only way* to protect the essential interest (see below). The greater the time lag between the discovery of the existence of the threat and its implementation, the more alternatives will generally be available to the injured state. This is also why the Tallinn Experts agreed that imminence in the context of plea of necessity has to be considered through the last "window of opportunity" standard applied in anticipatory self-defence.[217]

The Tallinn Manual 2.0 provides a number of examples of cyber operations for which the conditions of plea of necessity can be considered satisfied. These include "a cyber operation that would debilitate the state's banking system, cause a dramatic loss of confidence in its stock market, ground flights nation-wide, halt all rail traffic, stop national pension and other social benefits, alter national health records in a manner endangering the health of the population, cause a major environmental disaster, shut down a large electrical grid, seriously disrupt the national food distribution network, or shut down the integrated air defence system".[218]

Only mean

It is clearly stipulated in the art. 25 of ARSIWA, that the plea of necessity is available only if there is no other way "to safeguard that [essential] interest", notwithstanding that possible alternative solutions are "more costly or less convenient".[219] Such alternatives may be purely technical solutions (e.g. moving operations from the damaged infrastructure to other available infrastructure),[220] the use of diplomatic procedures (see retorsion above), solutions through

[214] ARSIWA, art. 25, p. 83, para. 15.
[215] SCHMITT: *Peacetime Cyber Responses*…, p. 138.
[216] Gabčíkovo-Nagymaros, para. 54.
[217] SCHMITT: *Peacetime Cyber Responses*…, p. 139; *see also* ARIMATSU and SCHMITT: *The Plea of Necessity*…, p. 1190 and SCHALLER: *Beyond Self-Defense and Countermeasures*…, p. 1636.
[218] SCHMITT: *Peacetime Cyber Responses*…, p. 136.
[219] ARSIWA, art. 25(1)(a), p. 83, para. 15; *see also* ARIMATSU and SCHMITT: *The Plea of Necessity*…, p. 1192;
[220] SCHMITT: *Peacetime Cyber Responses*…, p. 139.

international organizations (e.g. referring the matter to the UN Security Council)[221] or other procedures, such as those listed in the Cyber Toolbox of the European Union.[222]

It is the "only mean available" condition that most often prevents the invocation of plea of necessity.[223] Indeed, this was also the case in the repeatedly cited ICJ decision in Gabcikovo-Nagymaros, where the ICJ found that the "only means" condition was not met.[224] The ICJ reached the same conclusion in Wall Advisory Opinion.[225] Also, in the SolarWinds Operation case in 2020, the United States did not have the option of acting directly against Russia by reference to necessity, as other options were available.[226]

The importance of this condition is also evidenced by the fact that four of the six national positions mentioning plea of necessity explicitly or implicitly (by reference to the terms of Article 25 of ARSIWA) mention this condition. These are Japan,[227] the Netherlands,[228] Norway[229] and Switzerland.[230]

Impairment of other interests

Another condition limiting the availability of the plea of necessity is the prohibition of serious breach of the essential interest of another state or "the international community as a whole".[231] A prerequisite for a plea of necessity measure is not the attributability of the cyber operation to the state on whose territory the measure is to be carried out. Thus, it will often be a situation where the state of origin of the threat has no connection to the threat (for example, it is a cyber operation by an independent non-state actor). Therefore, unlike countermeasures and self-defence, the essential interest of that state must also be taken into account.[232] This idea is well captured by

---

221 ARSIWA, art. 25, p. 83, para. 15; SCHMITT: *Peacetime Cyber Responses…*, p. 141.
222 COUNCIL OF THE EUROPEAN UNION: *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response…*; *see also* SCHWEIGHOFER, E., BRUNNER, I. AND ZANOL, J. Malicious Cyber Operations, "Hackbacks" and International Law: An Austrian Example As a Basis for Discussion on Permissible Responses. *Masaryk University Journal of Law and Technology*, 2020, 14 (2), p. 252.
223 LAHMANN: *Unilateral Remedies to Cyber Operations…*, p. 216.
224 Gabčíkovo-Nagymaros, para. 55.
225 Wall Advisory Opinion, para. 140.
226 SCHMITT, M. *Top Expert Backgrounder: Russia's SolarWinds Operation and International Law*. [online] New York: Just Security [viewed 5 January 2022]. Available from: https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.
227 MINISTRY OF FOREIGN AFFAIRS OF JAPAN. *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations*. [online] [viewed 5 January 2022], p. 5. Available from: https://www.mofa.go.jp/files/100200935.pdf.
228 GOVERNMENT OF THE KINGDOM OF THE NETHERLANDS: *Appendix: International law….*, p. 7-8.
229 UN *Official compendium of voluntary national contributions...*, p. 73.
230 FEDERAL DEPARTMENT OF FOREIGN AFFAIRS OF SWITZERLAND. *Switzerland's position paper…*
231 ARSIWA, art. 15(1)(b).
232 Countermeasures and self-defence have their own limits, of course, which must be respected in their application, but these are very different from the plea of necessity.

Schmitt when he stated that "states are precluded from addressing necessity situations if doing so would place any other state in comparable peril".[233] The practical implication of this plea of necessity concept is that a victim state whose essential interest is in a "grave an imminent peril", even if that essential interest "is far more significant" than the essential interest of another state that might be threatened by a possible response, cannot implement any defensive action on the basis of a plea of necessity that might threaten that less important essential interest of another state.[234] However, a different interpretation of Article 25(1)(b) of ARSIWA is also strongly represented in the scholarly debate, according to which the balancing of essential interests on both sides is key and the plea of necessity is available in situations where the interest protected by virtue of its invocation is of a substantially higher value than the interest that may be impaired by the operation.[235]

Exclusion of invoking necessity

Invocation of the plea of necessity is explicitly ruled out in certain situations. It is the exclusion of the plea of necessity by another rule of international law and the situation where the state has contributed to the creation of the grave and imminent peril by its own conduct. [236]

In the first case, it is a situation where the use of necessity is excluded by a treaty (e.g. humanitarian conventions regulating *ius in bellum*) or other treaties contain their own plea of necessity regime which applies as *lex specialis* to the customary plea of necessity.[237] Necessity is not a peremptory norm of international law, and there is therefore nothing to prevent a contractual departure from the customary rule between the parties. The state is then obliged to respect this obligation and follow the special regime. Otherwise, it runs the risk of committing an internationally wrongful act by breaching an obligation arising from a treaty.

Invocation of the plea of necessity is also precluded in case the victim state has contributed to the peril by its own action or omission. The basic premise for assessing the contribution of a state is that any contribution is not sufficient, but it must be a contribution "sufficiently substantial and not merely incidental or peripheral".[238] One can agree with the Tallinn Experts' conclusion that a state's failure to protect its own cyberinfrastructure is not a sufficiently substantial contribution to

[233] SCHMITT: *Peacetime Cyber Responses…*, p. 253;
[234] ARIMATSU and SCHMITT: *The Plea of Necessity…*, p. 1193.
[235] LAHMANN: *Unilateral Remedies to Cyber Operations…*, p. 221.
[236] ARSIWA, art. 25(2).
[237] ARSIWA, art. 25, p. 84, para. 19; LAHMANN: *Unilateral Remedies to Cyber Operations…*, p. 225.
[238] ARSIWA, art. 25, p. 84, para. 20.

preclude the applicability of the plea of necessity.[239] However, Lahnemman's conclusion that states are bound by a duty of due diligence to maintain up-to-date security of their own cyberinfrastructure, and thus if a grave and imminent peril arises in connection with inadequate security of cyberinfrastructure, the state does not have the ability to apply the plea of necessity, seems questionable.[240] His conclusion does not adequately reflect the realities of cyberspace. First, it should be emphasized that malicious actors are always a step ahead of the victim and even the best cyber security in the world does not guarantee perfect protection. Secondly, the scale of cyber infrastructure in use in the public and private sectors and the limited capacity of the state to effectively ensure and enforce that the cyber security of these technologies is always up-to-date must also be taken into account. To accept such a strict interpretation of the plea of necessity conditions presented by Lahnemman would mean virtually eliminating plea of necessity as a justification for measures taken in the context of cyber operations.

2.3.2 Limitation of plea of necessity not mentioned in art. 25 of ARSIWA

States are limited in their right to invoke plea of necessity by two other conditions that are not explicitly mentioned in art. 25 of ARSIWA. These are the condition of the proportionality of the measure taken on the basis of plea of necessity and the prohibition on the use of plea of necessity as a justification for a violation of a peremptory norm of international law under article 26 of ARSIWA.

First, let's look at the condition of proportionality. Measures taken under the plea of necessity are justified only to the extent that they are necessary "for preserving the essential interest threatened".[241] It is worth quoting the relevant part of the ILC's commentary on ARSIWA 1980: "Any conduct going beyond what is strictly necessary [...] will inevitably constitute a wrongful act per se, even if the plea of necessity is admissible as regards the remainder of the conduct. In particular, it is self-evident that once the peril has been averted by the adoption of conduct conflicting with the international obligation, the conduct will immediately become wrongful if persisted in, even though it has not been wrongful up to that point."[242] Some authors have subsumed the proportionality aspect under the condition of "only means available", but such a subsumption is not appropriate.[243] While the 'only means' condition requires the selection of the

---

[239] SCHMITT: *Peacetime Cyber Responses…*, p. 140.
[240] LAHMANN: *Unilateral Remedies to Cyber Operations…*, p. 228.
[241] ARSIWA 1980 with commentaries, art. 33, pp. 49-50, para. 33.
[242] Ibid.
[243] See ARIMATSU and SCHMITT: *The Plea of Necessity…*, p. 1192; LAHMANN: *Unilateral Remedies to Cyber Operations…*, p. 218.

most appropriate of the alternatives, the assessment of proportionality should only be undertaken at the next step, once the means have been decided. Thus, if a plea of necessity hack back operation infringing on the sovereignty of another state is chosen as the appropriate (only) means to remove the threat, proportionality then requires an assessment of how to carry out the operation so as not to cause consequences more severe than necessary for preserving the essential interest. It follows that proportionality must be seen as a separate condition for the implementation of the plea of necessity. Similarly, a distinction is made between necessity (choice of means) and proportionality (proportionality to the aim pursued) as conditions of self-defence. [244]

Another condition limiting the repertoire of remedies available on the basis of plea of necessity can be found in Article 26 of ARSIWA, according to which "circustances precluding wrongfulness" including plea of necessity cannot justify a violation of a peremptory norm of international law.[245] The ILC then explicitly mentions three rules of international law, the justification of the violation of which on the basis of plea of necessity is excluded, namely the prohibition of the use of force, the prohibition of genocide and the prohibition of killing of prisoners of war.[246] Which other rules of international law are mandatory is left to further interpretation by the ILC.[247] It is surprising that despite such a clearly articulated prohibition, the possibility of the use of force on the basis of the plea of necessity is still debated.[248] It is clear that the option of justifying the use of force on the basis of plea of necessity was not considered during the drafting of ARSIWA; on the contrary, it was ruled out. Furthermore, it can be argued that exceptions to the prohibition on the use of force should be approached restrictively, since the objective of international law is to maintain peace and security, and the creation of exceptions to the prohibition on the use of force is undoubtedly contrary to this objective (which is also the main objective of the UN).

Nevertheless, further development of the debate on the limits of the use of force in cyberspace is to be expected, because as long as there is a "grey zone" of use of force, there is also the risk that what one state considers a non-forcible measure is a prohibited use of force for another. Such a situation inherently contains the risk of unintended escalation and it is therefore in the interest of the international community to pay attention to this issue.

---

[244] GRANT, BARKER: *Parry & Grant encyclopaedic dictionary*…, pp. 549 - 550.
[245] ARSIWA, art. 26.
[246] ARSIWA 1980, art. 33, p. 50, para. 37.
[247] Ibid.
[248] See e.g. SCHMITT: *Peacetime Cyber Responses*…, p. 140; VIDMAR, J. The Use of Force as a Plea of Necessity. *American Journal of International Law Unbound*, 2017, 111, pp. 301-306; ARIMATSU and SCHMITT: *The Plea of Necessity*…, pp. 1193-1194; LAHMANN: *Unilateral Remedies to Cyber Operations*…; SCHALLER: *Beyond Self-Defense and Countermeasures*…, p. 1621; BANNELIER, CHRISTAKIS: *Cyber-Attacks: Preventions-Reactions*…, p. 97.

2.4 Conclusion

Cyber operations are a phenomenon that affects every state, and the question of legal measures to suppress them is a fundamental issue of international law. Plea of necessity is one of the unilateral remedies available. In contrast to countermeasures and self-defence, its application is not premised on the attributability of the cyber operation to the state, which is why this legal instrument has received increasing attention in scholarly debate and state practice.[249] It is therefore somewhat surprising that no mention of this legal instrument can be found in the final report of the Group of Governmental Experts on Advancing responsible state behaviour in cyberspace (GGE) from July 2021[250] or in the output of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) from March 2021.[251]

The aim of the article was to highlight some problematic aspects of the application of plea of necessity in the context of cyber operations. The plea of necessity can be an elegant solution to the problem of attributability of cyber operations to the state, which opens up the possibility of adopting justified protective measures. On the other hand, however, it is important to bear in mind the high risk of abuse, which has been repeatedly highlighted by the ILC and the expert community. The possibility of justifying the use of force on the basis of the plea of necessity seems particularly dangerous. So far (2024), eight states including Czech Republic have officially announced their position on applicability of plea of necessity in cyberspace and all of them agreed that, under strict conditions, plea of necessity will be available.[252] It can be expected that more states with a similar position will be forthcoming, and efforts should therefore be made to define as precisely as possible the admissibility of the plea of necessity in cyberspace, because it is here to stay.

---

[249] LOTRIONTE: *Reconsidering the Consequences…*, p. 96; OHLIN, J., D. and MAY, L. *Necessity in International Law*. 1st ed. New York: Oxford University Press, 2016, p. 39.

[250] UNITED NATIONS. *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. [online]. Doc. A/76/135, 14 July 2021 [viewed 8 January 2022]. Available from: https://www.undocs.org/pdf?symbol=en/A/76/135.

[251] UNITED NATIONS. *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report*. [online]. Doc. A/AC.290/2021/CRP.2, 10 March 2021 [viewed 7 January 2022]. Available from: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf; UNITED NATIONS. *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Chair's Summary*. [online]. Doc. A/AC.290/2021/CRP.3, 10 March 2021 [viewed 7 January 2022]. Available from: https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

[252] CZECH REPUBLIC, *Position paper on the application of international law in cyberspace*. [online] [viewed 14 May 2024], p. 16. Available from: https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf.

3 Countermeasures against Cyber Operations: Moving forward?[253]

3.1 Introduction

International legal order, in contrast to national legal systems, lacks the superior authority responsible for the enforcement of legal obligations owed by its subjects.[254] Enforcement is mostly decentralized and states have to rely on measures of self-help, spanning from mere retorsion (an unfriendly, but legal act) to the use of force in self-defense.[255] Somewhere in between these two extremes lie countermeasures, defined by the International Law Commission (hereinafter "ILC") as acts "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."[256] In other words, a state whose right has been breached (injured state) by action or omission of another state (responsible state), is allowed to take such measures which would otherwise be contrary to international law in order to force the responsible state to "procure cessation and reparation".[257]

For example, if state A interferes with electoral processes in state B to push forward a candidate it prefers, it will be in breach of the principle of non-intervention. State B as the injured state would then be in a position to take measures otherwise contrary to its obligation owed to the responsible state, for instance, it could close its airspace for aircrafts from the responsible state in breach of a mutual aviation treaty because the illegality of this act would be precluded by the fact that it has been taken as a countermeasure against predeceasing illegal act by the responsible state. However, such measure would have to be in conformity with conditions stemming from international law for countermeasures, which will be discussed in detail below, and could only be used to induce the responsible state to cease the breach of law and, if reasonable, to provide reparation. Countermeasures cannot be used to punish the responsible state.[258]

---

[253] This paper was originally published in the International Comparative Law Review [SPÁČIL, J. Countermeasures against Cyber Operations: Moving forward?. *International Comparative Law Review*, 2023, 23(2), pp. 86 - 110]. Research was supported by the student project "International legal aspects of defense against cyber operations: retorsion and countermeasures" (IGA_PF_2022_004) of the Palacký University in Olomouc. The work was prepared under the supervision of prof. JUDr. Dalibor Jílek, CSc.

[254] BANNELIER, CHRISTAKIS: *Cyber-Attacks: Preventions-Reactions…*, p. 41; Putting aside the mostly ineffective enforcement mechanism of the United Nations, i.e. measures taken by the Security Council pursuant to Chapter VII of the Charter of the United Nations (UN Charter). These measures, while might materially be of the same kind as countermeasures, cannot be considered as countermeasures, because these measures are legal ab initio - SCHMITT et al: *Tallinn Manual 2.0...*, p. 114.

[255] MIRON, A. and TZANAKOPOULOS, A. Unilateral Coercive Measures and International Law. *The Left in the European Parliament*, 2022, 1(1), p. 16.

[256] ARSIWA, p. 128.

[257] ARSIWA, p. 128; The terms "injured state" and "responsible state" can be considered settled and will be respected in this thesis, *see* SCHMITT: *"Below the Threshold" Cyber Operations...*, p. 703.

[258] SCHMITT et al: *Tallinn Manual 2.0...*, p. 116.

This paper focuses mainly on the countermeasures in cyberspace (also "cyber countermeasures"), since a lot of questions remain unanswered as regards the application of international law in the cyber realm. In particular, the relationship between countermeasures and the principle of due diligence, the possibility of collective countermeasures, countermeasures against non-state actors operating abroad, or countermeasures crossing the threshold of the prohibited use of force. All of these issues will be addressed and hopefully, some light will be shed on them using and analyzing public statements by states and international organizations made in recent years in relation to using countermeasures in cyberspace.

3.2 Countermeasures in cyberspace

Countermeasures constitute a circumstance precluding wrongfulness, which has been codified in the Draft Articles on Responsibility of States for Internationally Wrongful Acts (hereinafter "ARSIWA").[259] Although the Draft Articles are of non-binding character, the criteria for the application of countermeasures set forth herein represent a generally accepted standard.[260] This is evidenced by the fact that they have also been adopted almost in full in the Tallinn Manual, which provides as a general rule that "a state may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that it is owed by another state".[261] However, this does not mean that the application of this legal instrument in the cyber context does not give rise to controversy.[262] Nevertheless, these seem to be fading into the background and there is a gradual shift in the debate from the question of "whether" countermeasures can be applied in cyberspace to the question of "how" to apply them. This shift is demonstrated by the fact that the latest report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (hereinafter "UN GGE Report 2021") adopted by the UN General Assembly includes the following formulation: "An affected state's response to malicious ICT activity attributable to another state should be in accordance with its obligations under (...) international law, including those relating to the settlement of disputes by peaceful means and internationally wrongful acts."[263]

---

[259] ARSIWA, p. 75.
[260] MIRON and TZANAKOPOULOS: *Unilateral Coercive Measures...*, p. 16.
[261] SCHMITT et al: *Tallinn Manual 2.0...*, p. 111.
[262] SCHMITT, M. N. The Sixth United Nations GGE and International Law in Cyberspace. *Justsecurity.org* [online]. 10 June 2021 [viewed 20 October 2023]. Available from: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.
[263] UN Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security n. A/176/135 of 14 July 2021, p. 9.

It is the reference to "internationally wrongful acts" that can then be interpreted as an indirect reference to countermeasures.[264]

However, the implementation of countermeasures is not, of course, a question of the arbitrariness of states, but can only be resorted to under a number of conditions that not only limit the general applicability of countermeasures, but also have a major impact on what specific measures can be taken.[265] Respect for these conditions leads to a reduction in the risk of unplanned escalation, limits the possibilities for abuse of the countermeasures and guarantees "international stability and security".[266] The second part of the article is devoted to their analysis. The conditions are divided into groups in accordance with the ARSIWA structure, i. e. material ("requirements of the situation") and procedural ("conditions of implementation").[267]

3.2.1 Material conditions

The basic prerequisite that must be fulfilled in order for countermeasures to be available to the injured state is the existence of an *internationally wrongful act attributable to the responsible state*.[268] Only in such a case, subject to the fulfilment of the other conditions analyzed below, can measures be taken which are themselves contrary to international law but whose wrongfulness is precluded precisely because they fulfil the definition of countermeasures.[269]

Attribution of a conduct to the responsible state

Attribution, i.e., establishing and proving the legal responsibility of a particular state for a cyber operation, is one of the main challenges of cyber law.[270] While in the case of a conventional operation, such as the firing of a missile from the territory of one state onto the territory of another state, there is usually a lot of concrete evidence of the originator of the attack, the situation is quite different for cyber operations. Not only is it a problem to trace the specific attacker (i.e. the device from which the operation was carried out, so-called technical attribution), but even if the injured state is successful in this step, the link between the responsible state and this attacker (legal

---

[264] SCHMITT: *The Sixth United Nations GGE*...
[265] SIMMONS, N. A Brave New World: Applying the International Law of War to Cyber-Attacks. *Journal of Law & Cyber Warfare*, 2014, 4(1), p. 69; *see also* HAATAJA: *Cyber Attacks and…*, p. 36; MIRON and TZANAKOPOULOS: *Unilateral Coercive Measures*..., p. 17.
[266] BANNELIER and CHRISTAKIS: *Cyber-Attacks: Preventions-Reactions*..., p. 47.
[267] ARSIWA, p. 129.
[268] ARSIWA, p. 129, art. 49 para. 1.
[269] MIRON and TZANAKOPOULOS: *Unilateral Coercive Measures*..., p. 2.
[270] HAATAJA: *Cyber Operations and Collective Countermeasures*..., p. 50.

attribution) must be proven.[271] Given that a significant part of cyber operations are carried out by non-state actors, this step can also be highly problematic.[272] Yet legal attribution of the cyber operation to the responsible state is a prerequisite for the implementation of countermeasures.[273] While technical attribution is primarily related to available evidence (IP addresses, location, etc.), legal attribution is a legal consideration based on articles 4 to 8 of ARSIWA, which regulate the rules for deriving legal responsibility of states for internationally wrongful acts. In general, states are responsible for the actions of their own authorities and armed forces, but may also be held responsible for the actions of non-state actors (e.g. private entities directed by the state), provided other conditions are met.[274]

As the perpetrators of cyber operations often actively try to hide their identity (spoofing), or conduct operations from or through the territory of third states, injured states are at risk of misattribution.[275] An example is the cyber operation carried out by North Korea against servers in South Korea in 2013, which used computers in forty countries.[276] It is clear that most, if not all, of these countries had nothing to do with this cyber operation. If an injured state misidentifies a responsible state and takes countermeasures against an innocent third state based on that misattribution, it may itself be committing an internationally wrongful act. The scholarly debate then turns to the question of whether this wrongfulness is affected by conduct in good faith. According to one group of scholars, acting in good faith makes countermeasures legal even against a third state.[277] Most authors, however, hold that good faith does not liberate the injured state of its legal responsibility.[278] The latter view is then the official position of both the International Law Commission and the Tallinn Manual 2.0.[279] The risk of misattribution is one of the reasons why countermeasures should be approached with caution, which is also emphasized in official positions of some states, such as Brazil or the United States.[280]

Another issue related to attribution is the burden of proof. Is the state implementing countermeasures obliged to provide prior evidence that the target state is indeed responsible for

---

271 BANNELIER and CHRISTAKIS: *Cyber-Attacks: Preventions-Reactions...,* p. 45.
272 SCHMITT: *"Below the Threshold" Cyber Operations...*, p. 708.
273 SCHMITT et al: *Tallinn Manual 2.0...,* p. 113.
274 SCHMITT: *Peacetime Cyber Responses…*, pp. 254-255.
275 SCHMITT et al: *Tallinn Manual 2.0...,* p. 115; *see also* HAATAJA: *Cyber Operations and Collective Countermeasures...*, p. 38.
276 SCHMITT: *"Below the Threshold" Cyber Operations...*, p. 708.
277 LOTRIONTE: *Reconsidering the Consequences…*, p. 95; SCHMITT: *"Below the Threshold" Cyber Operations...*, p. 727.
278 *See* SCHMITT: *Peacetime Cyber Responses...*, p. 254; BANNELIER and CHRISTAKIS: *Cyber-Attacks: Preventions-Reactions...,* p. 47; HAATAJA: *Cyber Operations and Collective Countermeasures...*, p. 50; HINKLE, K., C. Countermeasures in the cyber context: One more thing to worry about. *Yale Journal of International Law*, 2011, 37(Fall), p. 17; LAHMANN: *Unilateral Remedies to Cyber Operations…*, p. 140.
279 SCHMITT et al: *Tallinn Manual 2.0...,* rule 20, para. 16; ARSIWA, p. 130, para. 3.
280 UN *Official compendium of voluntary national contributions...*, p. 21; EGAN: *International Law and Stability….*

the malign cyber operation? It seems that current international law does not impose such a condition.[281] However, from the point of view of the legitimacy of the measures taken in the eyes of the international community, it is more than advisable that such evidence be made public, either before or after the implementation of countermeasures.[282] Indeed, the UN GGE Report 2015 states that "accusations of organizing and implementing wrongful acts brought against states should be substantiated".[283] Conversely, if there is a judicial review of countermeasures, depending on the judicial authority, the injured state will be required to produce evidence (meet burden of proof) at the level of "clear and convincing evidence".[284] This issue was then aptly described by Canada in its official statement when it stated that "[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".[285]

Breach of international obligation

Internationally wrongful act is an action or omission that is attributable to the responsible state and "constitutes a breach of an international obligation of the state".[286] It thus contains three elements, namely that it is (1) an act (2) attributable to the state and (3) in breach of international law.[287] The existence of an internationally wrongful act that violates a legal obligation owed to the injured state is a condition *sine qua non* for any countermeasure, as confirmed by the International Court of Justice (hereinafter "ICJ") in the Gabčíkovo-Nagymaros Project case.[288] Since the first element

---

[281] BANNELIER and CHRISTAKIS: *Cyber-Attacks: Preventions-Reactions...*, p. 47; *see also* LOTRIONTE: *Reconsidering the Consequences...*, p. 94.
[282] BANNELIER and CHRISTAKIS: *Cyber-Attacks: Preventions-Reactions...*, p. 47.
[283] UN Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security n. A/70/174 of 22 July 2015.
[284] CYBER TOOLKIT. Scenario 06: Cyber countermeasures against an enabling State. Cyberlaw.ccdcoe.org [online]. [viewed 22 October 2023]. Available from: https://cyberlaw.ccdcoe.org/wiki/Scenario_06:_Cyber_countermeasures_against_an_enabling_State; GEISS, R. and LAHMANN, H. Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention. In: ZIOLKOWSKI, K. (ed). *Peacetime Regime for State Activities in Cyberspace*. Tallinn: NATO CCD COE, 2013, p. 624.
[285] GOVERNMENT OF CANADA. International Law applicable in cyberspace, international.gc.ca [online]. [viewed 22 October 2023]. Avaiable from: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a9; similarly MINISTRY OF FOREIGN AFFAIR OF FINLAND: International law and cyberspace: Finland's national positions. Um.fi [online] [viewed 23 October 2023]. Available from: https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727.
[286] ARSIWA, p. 34, Article 2.
[287] SCHMITT: *Peacetime Cyber Responses...*, p. 253.
[288] ARSIWA, p. 130, para. 2; Gabčíkovo-Nagymaros, para. 83.

does not pose a problem in practice and the second has been discussed above, it is now necessary to focus only on the third defined element, i.e. breach of international obligation by the responsible state.

International obligations can stem from both customary international law (e. g. prohibition of the use of force, principle of non-intervention) and treaty law (e. g. mutual aviation treaty).[289] Violation of both types of obligations constitutes an internationally wrongful act. An example of such an act is the conduct of a cyber operation against a coastal state from a ship sailing in its territorial waters, which constitutes a violation of the innocent passage regime. Failure to respect the principle of due diligence may also constitute a breach of an international obligation, which will be discussed below.[290] However, the principle of sovereignty is the most susceptible to violation, as it applies to all cyber infrastructure located within the territory of a state, and therefore any cyber operation against that infrastructure may also constitute a violation of an international obligation.[291]

As already indicated above in the section dealing with the burden of proof, it is the injured state that carries out self-assessment as regard fulfillment of conditions of countermeasures. Therefore, it is also for the injured state to consider whether the responsible state has breached an international obligation owed to the injured state. If the injured state makes an erroneous judgment in this respect (i.e. if it considers the breach of international obligation to be a legal act of the other state or if it does not interfere with the rights of the injured state), it will itself bear responsibility for any breach of international law by its alleged countermeasure.[292]

Purpose

Countermeasures can only be implemented "in order to induce the responsible state to comply with its obligations under Part Two [of ARSIWA]".[293] This specifically means "to cease the internationally wrongful conduct, if it is continuing, and to provide reparation".[294] Reparation refers to the potential injury suffered by the injured state.[295] The term "injury" is to be understood in the sense of Article 31 ARSIWA as "any damage, whether material or moral, caused by the internationally wrongful act".[296]

---

[289] BANNELIER and CHRISTAKIS: *Cyber-Attacks: Preventions-Reactions...*, p. 42; SCHMITT: *"Below the Threshold" Cyber Operations...*, p. 704.
[290] SCHMITT: *"Below the Threshold" Cyber Operations...*, p. 704.
[291] Ibid.
[292] DELERUE, F. *Cyber operations and international law.* 1st ed. Cambridge: Cambdrige University Press, 2020, p. 438.
[293] ARSIWA, p. 130.
[294] Ibid.
[295] SCHMITT: *"Below the Threshold" Cyber Operations...*, p. 714.
[296] ARSIWA, p. 91, art. 31, para. 2.

Countermeasures are therefore not a means to punish the responsible state, but can only aim at correcting the illegal situation, providing compensation, returning to the *status quo* and possibly also providing guarantees from the responsible state.[297] If the measures taken pursued the objective of punishing the responsible state, they would not be countermeasures and the injured state would itself have committed an internationally wrongful act.[298] A related point is that countermeasures are permissible only if they can succeed in achieving permissible objectives. Otherwise, it would be mere retaliation not authorized by law.[299]

Unbreachable obligations

ILC listed a set of obligations which shall not be affected by the countermeasures in art. 50 of ARSIWA. These include the obligation to refrain from breaching the prohibition of threat or use of force, protection of fundamental human rights, obligations of humanitarian character prohibiting reprisals, other peremptory norms, other mutual dispute settlement procedure and the principle of inviolability of diplomatic premises.[300]

The possible forceful countermeasures and prohibition of the use of force will be thoroughly discussed below.

When it comes to fundamental human rights, there is a general consensus that not all human rights enshrined in, inter alia, international treaties fall into the category of "fundamental" rights that cannot be interfered with through countermeasures. The question of which rights should be included in this category is a matter of debate. The ILC refers to those human rights "which may not be derogated from in time of war or other public emergency".[301] Typically, these include the right to life, health or the prohibition of torture and slavery.[302] Also norms of humanitarian law, captured in particular by the Geneva Conventions and their additional protocols, cannot be breached by countermeasures.[303] These humanitarian rules are directly reflected in the crimes defined in the Rome Statute of the International Criminal Court.[304] In view of these rules, a cyber operation aimed at interrupting the supply of water and electricity to a medical facility, for example,

---

297 SCHMITT et al: *Tallinn Manual 2.0...*, p. 116; A thorough analysis of this issue is provided by LAHMANN: *Unilateral Remedies to Cyber Operations...*, pp. 180-187; *see also* DELERUE: *Cyber operations and international...*, p. 190.
298 SCHMITT et al: *Tallinn Manual 2.0...*, p. 116, *see also* MIRON and TZANAKOPOULOS: *Unilateral Coercive Measures...*, p. 3.
299 SCHMITT: *Top Expert Backgrounder: Russia's SolarWinds…*
300 ARSIWA, p. 131, art. 50; similarly, SCHMITT et al: *Tallinn Manual 2.0...*, p. 122.
301 ARSIWA, p. 132.
302 European Convention on Human Rights from 1950, Articles 2 (life), 3 (torture), 4 (slavery), 15 para. 2 (prohibition of derogation); *see also* SCHMITT et al: *Tallinn Manual 2.0...*, p. 123.
303 ARSIWA, p. 132.
304 Rome Statute of the International Criminal Court from 1998, Articles 5-8bis.

would be inadmissible.[305] A right which, on the other hand, cannot be subsumed under "fundamental" rights is the right to free and democratic elections.[306] At the same time, however, the above prohibition on violating fundamental human rights does not mean that countermeasures taken cannot have a negative impact on these rights, since such a strict interpretation of the prohibition on interference with these rights would preclude almost any countermeasure.[307]

In the context of cyber operations, the obvious risk is the interference with the right to privacy. The question is whether this right can be classified as a "fundamental" right.[308] The authors of the Tallinn Manual could not reach consensus on this point.[309] Although the right to privacy is undoubtedly one of the most important human rights, it is a right that can be interfered with in certain cases (e.g. in criminal proceedings).[310] At the same time, if we put the above-mentioned rights (life, health, etc.) and the right to privacy side by side, it is clear that the consequences of an interference with these rights are very different, both in terms of the severity of the interference with the individual's personal life and in terms of the possibility of redress or compensation. One may therefore be inclined to conclude that the right to privacy may be infringed by countermeasures, of course to a reasonable extent (see proportionality below).

A similar question to that of fundamental human rights relates to "other peremptory norms". Which rules of international law fall into this category? The word "other" obviously refers to the previous rules (art. 50 para. 1 letter a), b), c) ARSIWA), which include a number of peremptory norms. One of the "other" peremptory norms is undoubtfully the prohibition of genocide.[311] It should be emphasized that even "mere" incitement is a violation of this norm. Thus, one can easily imagine a cyber operation aimed at spreading disinformation and manipulating data, the very purpose of which is to incite genocide. Such operations cannot be considered legal countermeasure.[312]

Deciding whether a particular right or obligation falls under peremptory norms (jus cogens) is then important not only because it precludes countermeasures, but also because peremptory norms create an obligation *erga omnes*, i.e. towards all states, and their violation by one state could

---

[305] SCHMITT et al: *Tallinn Manual 2.0...,* p. 124.
[306] MIRON and TZANAKOPOULOS: *Unilateral Coercive Measures...*, p. 9.
[307] Ibid, p. 11.
[308] SCHMITT: *"Below the Threshold" Cyber Operations...*, p. 721.
[309] SCHMITT et al: *Tallinn Manual 2.0...,* p. 124; *see also* DELERUE: *Cyber operations and international...,* p. 451.
[310] European Convention on Human Rights from 1950, Article 8 para. 2.
[311] Convention on the Prevention and Punishment of the Crime of Genocide from 1948.
[312] SCHMITT: *"Below the Threshold" Cyber Operations...*, p. 722; SCHMITT et al: *Tallinn Manual 2.0...,* p. 124.

potentially allow for collective countermeasure.[313] A separate section of the text below is devoted to this topic.

Treaty limitations (and exclusions)

The right to take countermeasures does not have the status of peremptory norms and therefore the application of this instrument can be excluded by treaties.[314] It can be a bilateral or multilateral treaty. Typically, it will be the exclusion of the enforcement of obligations under the treaty through countermeasures and this regime will be replaced by another mechanism.[315] For example, the founding treaties of the European Union establish a specific regime for enforcing compliance with EU obligations.[316] This regime takes precedence over countermeasures.[317]

Temporary

The temporal character of countermeasures follows logically from their purpose. Countermeasures are not intended to lead to the establishment of a new permanent state of affairs, but are a temporary measure taken with a view to restoring the ordinary legal situation.[318] This means that countermeasures are to be terminated when they have fulfilled their purpose ("responsible state has complied with its obligations of cessation and reparation").[319] This therefore establishes the latest point in time until which countermeasures can last.

In terms of timing, attention should also be paid to when countermeasures can be started. Unlike the right of self-defence, international law does not operate with the concept of anticipatory countermeasures.[320] Thus, their implementation cannot be undertaken preventively, but can only be used in response to an already existing internationally wrongful act, as confirmed by the ICJ in the Gabčíkovo-Nagymaros Project judgment.[321] This, of course, also precludes countermeasures from being used as a means of deterrence.[322]

---

313 MIRON and TZANAKOPOULOS: *Unilateral Coercive Measures...*, p. 9.
314 ARSIWA, p. 129.
315 SCHMITT et al: *Tallinn Manual 2.0...,* p. 115.
316 ARSIWA, p. 133.
317 SCHMITT: *Peacetime Cyber Responses...*, p. 258.
318 ARSIWA, p. 131.
319 ARSIWA, p. 137.
320 LOTRIONTE: *Reconsidering the Consequences...*, p. 95; HAATAJA: *Cyber Operations and Collective Countermeasures...*, p. 37; LAHMANN: *Unilateral Remedies to Cyber Operations...,* p. 175.
321 SCHMITT et al: *Tallinn Manual 2.0...,* p. 118; Gabčíkovo-Nagymaros, para. 83.
322 SCHMITT: *"Below the Threshold" Cyber Operations...*, p. 715.

Based on the above, it can be concluded that an injured state that proceeds with cyber countermeasures must retain the technical capacity to terminate them the moment it achieves the legitimate objective pursued. Therefore, it is not possible, for example, to launch a malicious code (virus) programmed to destroy data into the responsible state's system as a countermeasure without the injured state having the capacity to deactivate the virus. Nor can countermeasures be used to justify pre-emptive cyber operations that violate another state's sovereignty or another rule of international law.

Reversibility

The ILC has commented on the topic of reversibility of countermeasures and so did the ICJ in its case law.[323] Countermeasures must be reversible, but this condition is not absolute.[324] Indeed, the relevant rule of ARSIWA speaks of the need to adopt countermeasures that "as far as possible" allow "resumption of the obligation in question".[325] The ILC itself then explains the use of the phrase "as far as possible" to mean that if the injured state has a choice of several appropriate and effective countermeasures, it should choose such measures as will allow the resumption of the performance of the suspended obligation.[326] In doing so, a distinction must be made between the reversibility of the measure itself (restoring respect for the international legal obligation) and the reversibility of the effects of the measure (repairing the damage caused by the countermeasures).[327] The requirement of reversibility relates only to the reversibility of the measure itself.

Therefore, reversibility cannot be seen as meaning that the injured state should in any way compensate for the losses incurred by the responsible state as a result of the countermeasures. For example, if the injured state chooses as a countermeasure a cyber operation against the critical financial infrastructure of the responsible state, thereby temporarily disabling it, it will undoubtedly cause financial losses on the part of the responsible state, but it will not be obliged to compensate for those losses.[328]

By the same token, while a number of countermeasures may deprive the responsible state of the opportunity to carry out certain activities, which may harm it in an irreversible way, this does not mean that such measures are *a priori* excluded.[329]

---

[323] ARSIWA, p. 131; Gabčíkovo-Nagymaros, para. 87.
[324] ARSIWA, p. 131.
[325] Ibid, p. 129.
[326] ARSIWA, p. 131.
[327] LAHMANN: *Unilateral Remedies to Cyber Operations...,* p. 122.
[328] BANNELIER and CHRISTAKIS: *Cyber-Attacks: Preventions-Reactions...,* p. 42.
[329] HAATAJA: *Cyber Operations and Collective Countermeasures...*, p. 38; SCHMITT et al: *Tallinn Manual 2.0...,* p. 119.

Proportionality

For proportionality ARSIWA contains a special rule: "Countermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[330] The question of proportionality of countermeasures was also addressed by the ICJ in the Gabčíkovo-Nagymaros case.[331] The ILC Commentary further specifies that "proportionality must be assessed taking into account not only the purely 'quantitative' element of the injury suffered, but also 'qualitative' factors such as the importance of the interest protected by the rule infringed and the seriousness of the breach".[332] In doing so, it is necessary to take into account not only the breached right of the injured stated, but also the right of the responsible state which will be affected by the countermeasures.[333] Injury in this context does not necessarily refer to any material damage, but is the very violation of the right of the injured state.[334] In other words, proportionality in the context of countermeasures must be assessed in relation to the injury caused, and the injury caused by the countermeasures must not significantly exceed the injury caused by the conduct of the responsible state.[335]

The aspect of proportionality is very abstract. Proportionality has to be assessed on a case-by-case basis.[336] However, the key point is that proportionality in no way implies reciprocity in the sense of using the same means or targeting against the same right.[337] Thus, for example, a restriction on the right of innocent passage in the form of a naval blockade may be responded to by a cyber operation directed against the sovereignty of the responsible state and vice versa.

It should further be emphasized that the proportionality of countermeasures is a concept distinct from proportionality in the right of self-defense.[338] In the case of countermeasures, the comparative criterion is not the necessity of the measure to achieve the objective pursued (cessation and reparation), but proportionality in relation to the injury caused.[339] Thus, whereas in self-defense the consequences of the measures taken may cause significantly greater harm than that caused by the armed attack which activated the right of self-defense, if this is necessary to prevent a further armed

---

330 ARSIWA, p. 134.
331 Gabčíkovo-Nagymaros.
332 ARSIWA, p. 135.
333 Ibid.
334 SCHMITT et al: *Tallinn Manual 2.0...,* p. 127.
335ARIMATSU and SCHMITT: *The Plea of Necessity…*, p. 1180.
336 CYBER TOOLKIT: *Scenario 06...*
337 BANNELIER and CHRISTAKIS: *Cyber-Attacks: Preventions-Reactions...,* p. 49; *see also* SCHMITT et al: *Tallinn Manual 2.0...,* p. 128 and HINKLE: *Countermeasures in the cyber context...*, p. 20.
338 SCHMITT: *"Below the Threshold" Cyber Operations...*, p. 723.
339 ARIMATSU and SCHMITT: *The Plea of Necessity...*, p. 1181.

attack, in countermeasures the condition of proportionality is more stringent and may lead to the situation that, although the injured state would have the means available to achieve the objective pursued, it will not be able to use them because the injury caused by them will be disproportionate in relation to the injury suffered.

Similarly, proportionality of countermeasures should be distinguished from the concept of proportionality in humanitarian law.[340]

It is impossible to fully estimate and control impact of cyber countermeasures on the responsible state (and possibly also third states).[341] By comparison, if as a countermeasure the airspace of an injured state is closed to aircrafts registered in a responsible state, the consequences of such a measure (number of flights affected, economic impact,...) can be estimated quite accurately. On the other hand, if malware is used as a countermeasure and released into the responsible state's network with the aim of removing important data, it is often not possible to estimate the extent to which the data will be damaged and whether unplanned spread of the malware beyond the target facilities will occur and thus lead to a more significant interference with the rights of the responsible state, given the limited level of control and planning. From the above, it is clear that cyber countermeasures entail a significant risk of unintentional overreach and their use requires a high degree of prudence on the part of the injured state.

Necessity

Necessity is closely linked to the purpose and the proportionality of countermeasures. Countermeasures are available only if they are necessary to achieve the purpose of cessation and reparation.[342] In order to conclude that countermeasures are indeed necessary, the injured state must comply with Article 52 of ARSIWA, which contains the procedural conditions for their application. This means in particular to make a "prior demand" that the responsible state ends the breach of international obligation and an offer to negotiate.[343] Only if, even in response to this demand, the responsible state does not put an end to the unlawful situation, does it open the way for countermeasures. However, these procedural conditions can be omitted in the case of so-callled urgent countermeasures (see below).[344]

---

340 SCHMITT et al: *Tallinn Manual 2.0...,* p. 127.
341 Ibid, p. 128; *see also* HAATAJA: *Cyber Operations and Collective Countermeasures...*, p. 40.
342 HINKLE: *Countermeasures in the cyber context...*, p. 18.
343 HINKLE: *Countermeasures in the cyber context...*, p. 18; ARSIWA, p. 135.
344 ARSIWA, p. 135.

3.2.2 Procedural conditions

So far we have been dealing with material conditions. However, countermeasures are also constrained by several procedural requirements, by which we must understand the concrete steps in relation to the responsible state that must precede countermeasures. These are (1) an obligation to request cessation of the internationally wrongful act and/or provide reparation[345] and (2) "to notify the responsible state of any decision to take countermeasures and [3] offer to negotiate with that state".[346] Compliance with these conditions is a prerequisite for the legality of subsequent countermeasures.

While the necessity to request the responsible state to terminate the unlawful situation must be insisted upon even in the context of cyber countermeasures (especially for reasons of possible "spoofing", i.e. masking the real originator),[347] the other two conditions (to notify, to negotiate) can exceptionally, according to the prevailing opinion,[348] be waived with reference to so-called urgent countermeasures if it is "necessary to preserve [the injured state's] rights".[349] These "rights" include both the rights violated and the right to take countermeasures.[350] The main reason why prior notification to the responsible state of planned cyber countermeasures may be problematic is that the responsible state could subsequently take measures that would reduce or eliminate the effectiveness of such cyber countermeasures altogether.[351] Conversely, one cannot agree with the view of Katharine Hinkle, according to whom the case for urgent countermeasures is also supported by the fact that "were the perpetrating state to receive notice [...] it could easily 'immunize' itself [...] by ending the cyber-assault".[352] Indeed, the author overlooks that the possibility of ending the wrongful act by the responsible state is the very reason why the state is notified. As noted above, this procedural condition is a corollary of the material condition of necessity.

On the other hand, however, it cannot be overlooked that not all states accept the view that urgent countermeasures can be undertaken without prior notification. Canada for example considers that procedural aspects of countermeasures, including notification, need "to be further defined through

---

345 Gabčíkovo-Nagymaros, para. 84.
346 ARSIWA, p. 135.
347 HAATAJA: *Cyber Operations and Collective Countermeasures...*, p. 38.
348 Group of Experts which prepared the Tallinn Manual agreed that "may launch urgent countermeasures without notification". *See* SCHMITT et al: *Tallinn Manual 2.0...,* p. 120.
349 Ibid.; For thorough analysis see also LAHMANN: *Unilateral Remedies to Cyber Operations...,* pp. 121, 138; DELERUE: *Cyber operations and international...,* pp. 444-445.
350 Ibid.
351 SCHMITT et al: *Tallinn Manual 2.0...,* p. 120; SCHMITT: *Peacetime Cyber Responses...*, p. 257.
352 HINKLE: *Countermeasures in the cyber context...*, p. 19.

state practice given the unique nature of cyberspace".[353] However, the prevailing view, even among states (France,[354] Israel,[355] Italy,[356] Netherlands,[357] Norway,[358] Sweden,[359] United States[360] or United Kingdom[361]) is that urgent countermeasures without prior notification can be taken, particularly in cyberspace. At the same time, however, these states stress that this is an exception to the general notification obligation, which remains an established procedural condition of countermeasures.

These procedural conditions balance the "self-appreciation" of the fulfilment of the material conditions by the injured state,[362] reduce the risk of unplanned escalation and prevent misattribution.

3.3 Contentious issues

While the first part of the text was devoted to countermeasures in general, the conditions of their admissibility and the relationship between this legal instrument and cyberspace, the second part will focus on the contentious issues associated with countermeasures. These are the link between countermeasures and the principle of due diligence, countermeasures and the use of force and finally the question of collective countermeasures.

3.3.1 Countermeasures and due diligence

It has already been mentioned that one of the main practical obstacles to countermeasures is the requirement to legally attribute the conduct (which breaches the international law) to a particular state. Unless this requirement is fulfilled, there is no space to launch countermeasures.[363] This

---

353 GOVERNMENT OF CANADA: *International Law applicable in cyberspace...*
354 MINISTRY OF DEFENCE OF FRANCE: *International Law Applied to Operations* ….
355 SCHÖNDORF, R. Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations. *International Law* Studies, 2021, 97(1), p. 405.
356 ITALY. *Italian Position Paper on `International Law and Cyberspace`*. Esteri.it [online]. [viewed 3 November 2023]. Available from: https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf.
357 GOVERNMENT OF THE KINGDOM OF THE NETHERLANDS: *Appendix: International law…..*
358 UN *Official compendium of voluntary national contributions...*, pp. 72 - 73.
359 GOVERNMENT OFFICES OF SWEDEN. Position Paper on the Application of International Law in Cyberspace. *Regeringen.se* [online]. July 2022 [viewed 3 November 2023]. Available from: https://www.regeringen.se/4a1ce0/contentassets/2bf3882c23bb4fdfb935310b03d562a1/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf.
360 UN *Official compendium of voluntary national contributions...*, p. 142.
361 GOVERNMENT OF THE UNITED KINGDOM. Cyber and International Law in the 21st Century. Gov.uk [online]. 23 May 2018 [viewed 3 November 2023]. Avaiable from: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
362 MIRON and TZANAKOPOULOS: *Unilateral Coercive Measures...*, p. 18.
363 SCHMITT, M., N. and WATTS, S. Beyond State-Centrism: International Law and Non-State Actors in Cyberspace. *Journal of Conflict & Security Law*, 2016, 21(3), p. 12.

means that even if an injured state has sufficient evidence that a cyber operation is being conducted from the territory of a particular state, it may not be able to infer the legal responsibility of that state. However, this very situation may open the door for countermeasures for breach of the due diligence principle.

Due diligence means that each state has an obligation "not to allow knowingly its territory to be used for acts contrary to the rights of other states".[364] However, it must be stressed that the existence of this rule in customary international law is controversial and the practice of states is fragmented in this respect.[365] It is not the subject of this article, however, to examine the existence of this rule and, since it has been incorporated into the text of the Tallinn Manual 2.0 (rule 6), it will continue to be assumed that states do have such an obligation under international law.[366]

Applied in cyberspace, then, the obligation of due diligence implies the obligation of the territorial state (the state from whose territory the cyber operation is carried out) to prevent the execution of that operation if it becomes aware of it (or should have become aware of it).[367] This is not a obligation of prevention, but an obligation to act, so there is no need to take any precautionary measures or to monitor one's own cyber infrastructure.[368] An example is when a terrorist organization misuses cyber infrastructure on the territory of a state to attack another state and the attacked state informs the territorial state of the attack. The state is then obliged to take action, within its capabilities, against the terrorist activity. The principle of due diligence does not require that the intervention be effective, but it must be within the capabilities (especially technical capabilities) of the territorial state ("take all feasible measures").[369] A territorial state that does not have sufficient technical capability to stop a cyber operation cannot therefore be responsible for a breach of the principle of due diligence.[370] If a territorial state does not act in accordance with due diligence, even though it has the technical capacity, it is itself in breach of international law (committing an internationally wrongful act) and thus runs the risk of countermeasures being used against it.

---

[364] *Corfu Channel Case (UK v Albania)*, ICJ, Judgement, 9 April 1949, para. 22 (hereinafter „Corfu Channel").
[365] For a thorough analysis of the positions of individual states, see CYBER TOOLKIT: *Scenario 06...*; *see also* ARIMATSU and SCHMITT: *The Plea of Necessity...*, p. 1180.
[366] SCHMITT et al: *Tallinn Manual 2.0...,* rule 6; A thorough analysis of the due diligence principle is offered by LAHMANN: *Unilateral Remedies to Cyber Operations...,* pp. 155-163.
[367] SCHMITT et al: *Tallinn Manual 2.0...,* rule 6; SCHMITT and WATTS: *Beyond State-Centrism...*, p. 12; SCHMITT: *Peacetime Cyber Responses...*, p. 259; BANNELIER and CHRISTAKIS: *Cyber-Attacks: Preventions-Reactions...,* pp. 44-45; SCHMITT: *"Below the Threshold" Cyber Operations...*, p. 706.
[368] SCHMITT et al: *Tallinn Manual 2.0...,* rule 6; SCHMITT: *Peacetime Cyber Responses...*, p. 259; SCHMITT, M., N. Terminological Precision and International Cyber Law. *Lieber.westpoint.edu* [online]. 29 July 2021 [viewed 3 November 2023]. Available from: https://lieber.westpoint.edu/terminological-precision-international-cyber-law/.
[369] SCHMITT et al: *Tallinn Manual 2.0...,* p. 130.
[370] SCHMITT: *Peacetime Cyber Responses...*, p. 260.

In such a situation, the injured state has two options how to approach countermeasures. The first way is to use countermeasures against the territorial state (its authorities) and thus force it to take action against a terrorist cyber operation.[371] The second, and arguably more effective remedy, is direct action against a terrorist operation on the territory of the territorial state.[372] The second option will in fact constitute a violation of the territorial state's sovereignty, but the illegality of this action will be precluded precisely by the fact that it will be a countermeasure. Particularly in the case of direct intervention, then, care must be taken to ensure that the threshold of the use of force or armed attack is not crossed (see below).

In this context, the rule of proportionality should be recalled and emphasized. As explained, countermeasures have to be proportionate to the injury suffered. In the case of a breach of the principle of due diligence, it is the breach of due diligence ("the failure to take appropriate measures") and not the (cyber or other) operation itself that is the injury.[373] Therefore, the countermeasure taken must be proportionate to the breach of due diligence and not to the consequences of the operation itself.[374] This will often mean that the injured state will not have available a sufficiently effective countermeasures because such measures would be disproportionate. In such a situation, it may be appropriate to consider other measures on the basis of, for example, plea of necessity, other circumstances precluding wrongfulness.[375]

3.3.2 Forcible countermeasures

Article 50(1)(a) of ARSIWA provides that "Countermeasures shall not affect the obligation to refrain from the threat or use of force" as stipulated in the Charter of the United Nations.[376] Yet the possibility of countermeasures crossing the threshold of the use of force remains an open question.[377] In particular, the fact that the right of self-defense, otherwise one of the few exceptions to the prohibition on the use of force, is only available to states when an "armed attack" occurs opens up space for this debate.[378] Armed attacks are cases of serious violation of the prohibition on the use of force.[379] Thus, there are acts that, while constituting a violation of the prohibition of

---

[371] SCHMITT: *Peacetime Cyber Responses...*, p. 259.
[372] Ibid.
[373] SCHMITT et al: *Tallinn Manual 2.0...,* p. 130.
[374] SCHMITT and WATTS: *Beyond State-Centrism...*, p. 12.
[375] A comprehensive analysis of plea of necessity in the context of cyber operations: ARIMATSU and SCHMITT: *The Plea of Necessity...* or SPÁČIL, J. Plea of Necessity: Legal Key to Protection against Unattributable Cyber Operations. *Masaryk University Journal of Law and Technology*, 2022, 16(2), pp. 215-239.
[376] Charter of the United Nations from 1945, Article 2 para. 4.
[377] SCHMITT et al: *Tallinn Manual 2.0...,* p. 112.
[378] Charter of the United Nations from 1945, Article 51.
[379] Nicaragua v. United States, para. 191.

the use of force, do not rise to the level of an armed attack.[380] Even so, they are of course violations of international law, which opens the door to countermeasures. And it is here that the question arises whether these specific violations of the prohibition of the use of force below the armed attack threshold could be defended against by countermeasures of the same intensity (i. e., use of force but below the armed attack threshold).[381]

In this context, it should be also pointed out that it is problematic to determine which cyber operations reach the intensity of use of force or armed attack.[382] Doubts exist in particular in the case of operations against critical infrastructure.[383] A related problem is the limited ability to estimate the actual impact of a cyber operation, which may thus cross the threshold of not only use of force but also armed attack accidentally.[384]

The prevailing view is that even against these less potent uses of force below the threshold of an armed attack, countermeasures of equal intensity cannot be used. This view follows not only from ARSIWA but also from the case law of the ICJ and is held by most experts.[385] The main argument of the proponents of the opposite approach, then, is that if the injured state were to be victimized by a use of force (cyber or not) below the armed attack threshold, it could not afford to defend itself in a similar manner, although it is generally entitled to a proportionate response.[386] In support of this position, these authors often refer to the separate opinion of Judge Simma in the Oil Platforms Case, which they interpret in favour of forcible countermeasures.[387]

While one can understand the arguments for both approaches, the more restrictive approach of not allowing forcible countermeasures seems more convincing.

In legal terms, the arguments on the side of the opponents of forcible countermeasures are generally stronger. This is not only the aforementioned ICJ case law and the enshrinement of the rule in ARSIWA, but in particular the prohibition on the use of force in the UN Charter must be taken into account. As a peremptory norm of international law, arguably one of the most important

---

[380] We leave aside the fact that some states, in particular the United States, take the view that any use of force is an armed attack. On the "gap" see also LAHMANN: *Unilateral Remedies to Cyber Operations...,* pp. 129-130.
[381] SCHMITT et al: *Tallinn Manual 2.0...,* p. 125.
[382] BANNELIER and CHRISTAKIS: *Cyber-Attacks: Preventions-Reactions...,* p. 48; ROSCINI, M. *Cyber Operations and the Use of Force in International Law*. 1st ed. New York: Oxford University Press, 2016, p. 250; LOTRIONTE: *Reconsidering the Consequences...*, p. 95.
[383] *See* SPÁČIL, J. Cyber Operations against Critical Financial Infrastructure: a Non-Destructive Armed Attack?. *International and Comparative Law Review*, 2022, 22(2), pp. 27-42.
[384] SIMMONS: *A Brave New World...*, p. 71.
[385] Corfu Channel, para. 35; Nicaragua v. United States, para. 249; Forcible countermeasures are also opposed by most expert compilers (see SCHMITT et al: *Tallinn Manual 2.0...,* p. 125).
[386] SCHMITT et al: *Tallinn Manual 2.0...,* p. 126.
[387] *Oil Platforms (Islamic Republic of Iran v. United States of America)*, ICJ, Judgement, 12 December 1996, separate opinon of Judge Simma, para. 13; SCHMITT et al: *Tallinn Manual 2.0...,* p. 126.

norms, which can be derogated from only exceptionally on the basis of the right of self-defense or with the consent of the UN Security Council, it deserves the highest degree of caution when establishing exceptions to it (restrictive approach). The proponents of forcible countermeasures have put forward completely insufficient arguments from this perspective. Although Judge Simma is undoubtedly one of the greatest authorities on international law, his one dissenting opinion cannot be equated with the opinions of the ICJ, ILC and the UN Charter.

There are also purely pragmatic arguments against forcible countermeasures. In particular, the risk of escalation.[388] It is not possible to clearly define which minor act already fulfils the characteristics of an armed attack.[389] This problem becomes even more pronounced in the cyber context (for example, it is not clear whether the mere destruction of data can constitute a use of force or not).[390] Allowing the use of force as a countermeasure in response to such ambiguously classified actions may lead to a more intense counter-reaction by the responsible state, and it is not difficult to imagine a gradation to the level of armed attack and subsequent armed conflict.

Finally, the recent practice of states in the form of official national positions on applicability of international law in cyberspace is quite uniform. Australia, Canada, Finland, France, Italy, Netherlands, New Zealand, Norway, Sweden, Switzerland, United States, United Kingdom and even Russia have opposed the possibility of justifying any use of force on the basis of countermeasures.[391] These are overwhelmingly post-Tallinn Manual 2.0 opinions, and if a minority of experts in this publication lean towards the possibility of forcible countermeasures, it seems safe to conclude that this possibility is indeed ruled out, taking into account this subsequent state practice.

On the basis of all these arguments, it can therefore be concluded that forcible countermeasures are completely out of the question, and unless there is a fundamental change in state practice, which does not seem likely, this debate can be considered essentially closed, at least in cyberspace.

---

388 *See* MIRON and TZANAKOPOULOS: *Unilateral Coercive Measures...*, p. 30; HAATAJA: *Cyber Operations and Collective Countermeasures...*, p. 51; SCHMITT: *"Below the Threshold" Cyber Operations...*, p. 715.
389 SCHMITT: *"Below the Threshold" Cyber Operations...*, p. 719.
390 HAATAJA: *Cyber Operations and Collective Countermeasures...*, p. 39.
391 For overview of national positions on this topic see https://cyberlaw.ccdcoe.org/wiki/Countermeasures.

3.3.3 Collective countermeasures

While the right to collective self-defense is enshrined directly in the UN Charter,[392] the status of a similar rule for countermeasures in international law is unclear and controversial.[393] Although examples of collective countermeasures have appeared throughout history, the ILC refers to them as "controversial" and "embryonic".[394] Yet, this issue is significant in the context of cyber operations, as many states do not possess sufficient technical capacity to be able to implement effective cyber countermeasures on their own.[395] At the same time, there is a relatively well-developed international cooperation in the field of cyber operations (e.g. NATO Rapid Reaction Team)[396] and it is therefore necessary to examine what are the limits of cooperation between states, whether third states can assist the injured state in implementing countermeasures or even implement it fully on its behalf.

There are several perspectives on collective countermeasures, which are clearly summarised in the commentary to rule 24 of the Tallinn Manual 2.0. According to the final version of this rule "only an injured state may engage in countermeasures".[397] However, the commentary reveals the complexity of the problem. Several experts took the position that a non-injured state may implement countermeasures on behalf of an injured state on the request of that state.[398] The majority, however, was opposed.[399] Even more fragmented then was the debate on the possibility of mere assistance by the injured state.[400] The structure of the debate is similar in the broader context. Some authors strictly reject collective countermeasures,[401] while others see limited scope for their implementation.[402]

Schmitt and Watts thoroughly analyzed the issue of cyber countermeasures in 2021 and concluded that "collective cyber countermeasures ... are lawful." They support this conclusion by noting that there is no clear prohibition of collective countermeasures in international law, international law generally tends towards a "collectivist approach", the specific nature of cyberspace requires a

---

392 Charter of the United Nations from 1945, Article 51.
393 SCHMITT: *The Sixth United Nations GGE...*; OSULA, A., KASPER, A. and KAJANDER, A. EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 2022, 16(1), p. 105.
394 ARSIWA, p. 129.
395 SIMMONS: *A Brave New World...*, p. 70.
396 NATO. Men in black - NATO's cybermen. *Nato.int* [online]. 24 April 2015 [viewed 4 November 2023]. Available from: https://www.nato.int/cps/en/natohq/news_118855.htm.
397 SCHMITT et al: *Tallinn Manual 2.0...,* p. 130.
398 Ibid, p. 132.
399 Ibid.
400 Ibid.
401 SIMMONS: *A Brave New World...*, p. 70.
402 SCHMITT, M., N. and WATTS, S. Collective Cyber Countermeasures?. *Harvard National Securitys Journal*, 2021, 12(1), p. 213; SCHMITT, M., N. Expert Backgrounder: NATO Response Options to Potential Russia Cyber Attack. *Justsecurity.org* [online]. 24 February 2022 [viewed 4 November 2023]. Available from: https://www.justsecurity.org/80347/expert-backgrounder-nato-response-options-to-potential-russia-cyber-attacks/.

greater degree of tolerance of countermeasures, and allowing collective countermeasures is fully consistent with the "object and purpose of the rule of countermeasures".[403] However, this conclusion still seems too strong compared to recent state practice.

Estonia is the only country that explicitly and unequivocally takes the position that collective countermeasures are legal.[404] New Zealand, the United Kingdom and Poland are less explicit, but still in favour of collective countermeasures.[405] On the other hand, France takes a completely negative position and Canada considers that there is not yet sufficient "state practice and opinion juris" for collective countermeasures.[406]

On the basis of all the above, it can be concluded that Catherine Lotrionte's conclusion expressed in 2018, that the issue "has yet to be resolved, leaving open the further development of the law through state practice and opinion juris and the possibility for collective, or third-party, cyber countermeasures" remains valid.[407] At the same time, however, it must be acknowledged that both expert debate and state practice are moving towards an increasing tolerance of collective countermeasures, at least in cyberspace. Unless this trend changes, we can expect this new dimension of countermeasures in customary international law to stabilize in the coming years.[408]

3.4 Conclusion

Countermeasures constitute a circumstance precluding wrongfulness that may allow the injured state to effectively protect its own rights. However, the applicability of this concept of international law is limited by a number of material and procedural conditions that must be insisted upon.

The aim of this article was to explore the possibilities of applying countermeasures in cyberspace and in particular to take into account recent state practice and development in scholarly debate. It is clear that this instrument has received considerable attention from both states and scholars. This

---

403 SCHMITT and WATTS: *Collective Cyber Countermeasures…*

404 UN *Official compendium of voluntary national contributions...*, p. 28.

405 DEPARTMENT OF THE PRIME MINISTER AND CABINET, NEW ZEALAND. *The Application of International Law to State Activity…*; BRAVERMAN: *International Law in Future Frontiers…*; MINISTRY OF FOREIGN AFFAIRS OF POLAND. The Republic of Poland's position on the application of international law in cyberspace. Gov.pl [online]. 29 December 2022 [viewed 4 November 2023]. Available from: https://www.gov.pl/attachment/3203b18b-a83f-4b92-8da2-fa0e3b449131.

406 MINISTRY OF DEFENCE OF FRANCE. *International Law Applied...*; GOVERNMENT OF CANADA: *International Law applicable in cyberspace...*

407 SCHMITT and WATTS: *Collective Cyber Countermeasures...*, p. 213.

408 Given the limited scope of this work, it is no longer possible to address countermeasures based on a violation of the erga omnes prohibition. However, this issue has been dealt with very thoroughly by other authors, and reference may be made to the following materials: HAATAJA: *Cyber Operations and Collective Countermeasures...*, pp. 41-49; SCHMITT et al: *Tallinn Manual 2.0...*, p. 130; SCHMITT and WATTS: *Collective Cyber Countermeasures...*, pp. 176-214; SCHMITT: *"Below the Threshold" Cyber Operations...*, pp. 728-729; DELERUE: *Cyber operations and international...*, pp. 454-456.

paper described some of the apparent trends relating to the application of countermeasures in cyberspace.

In general, it can be stated that there can no longer be any doubt that countermeasures are also applicable in cyberspace, but in this context one of the main obstacles to their application remains the need to attribute the malign conduct (cyber operation) to the responsible state. Compliance with the proportionality requirement in the case of cyber countermeasures may also be a specific challenge due to the limited predictability of the consequences of such a cyber operation and its controllability. Regarding procedural conditions, it is necessary to highlight in particular the growing support for urgent countermeasures not requiring prior notification of the responsible state.

In the second part of the article, attention was paid to the contentious issues associated with countermeasures.

The principle of due diligence, respectively its violation by a territorial state, can open the door to countermeasures targeting not only that state, but also directly against non-state actors operating from its territory. It is precisely through the violation of due diligence that it is possible to circumvent the condition of attributability of the state's actions (in relation to malign cyber operations), which can be quite crucial for the injured state.

In the next section, based on an analysis of state practice, the opinion was presented that while the Tallinn Manual 2.0 still allowed the theoretical possibility that international law could permit limited forcible countermeasures against the use of force under the armed attack threshold, developments in recent years have essentially ruled out this alternative, as there is no single state that would allow such a possibility and, on the contrary, at least 12 states, including the US and Russia, have ruled out forcible countermeasures (in cyberspace).

The last segment was dedicated to collective countermeasures. The possibility of their implementation remains controversial, but in recent years there has been growing support for them both in academia and in state practice. Unless this trend changes, collective countermeasures may soon become a stable part of international law.

Conclusion

Within this thesis, attention has been paid to three important instruments of international law that can justify retaliatory responses to hostile cyber operations - retorsion, plea of necessity and countermeasures.

The first chapter discussed retorsion as unfriendly, but legal conduct. Retorsion is the least researched of the three instruments analysed, but this has been changing in recent years. Retorsion is not only coming into focus in academic debate, but is also slowly returning to the vocabulary of states, as evidenced by the many mentions in the official documents and statements that were analysed. Given that most of the measures taken by states in response to cyber operations directed against other states had the nature of retorsion, this trend can be expected to continue.

The interaction between states in cyberspace has not only created room for a return to traditional retorsion measures, but has also given rise to entirely new measures (cyber retorsion), such as restricting access to one's own cyber infrastructure or warning individuals responsible for conducting cyber operations.

Retorsion is the most versatile of the three instruments described, as retorsion measures are subject to almost no restrictions (provided they do not violate any other rule of international law) and can be used against any state regardless of whether its international legal responsibility for the cyber operation has been proven. Although these measures are generally less effective, they certainly have a strong place in the defense against malign cyber operations.

Like retorsion, plea of necessity has the great advantage that its application does not presuppose legal attribution of the conduct to the target state. At the same time, however, it also allows for a considerably wider range of measures that may be contrary to the norms of international law, since it is a condition precluding wrongfulness. This advantage is balanced, on the other hand, by the strict conditions that must be met in order for a measure to be acceptable under this instrument. An analysis of these conditions forms sizeable part of the relevant chapter.

While in the past, self-defence was the main focus in the defence against cyber operations, today less invasive and more practical legal instruments, including the plea of necessity, are gaining prominence. This trend is likely to continue, as confirmed by the newly published national position

of the Czech Republic on application of international law in cyberspace (February 2024), which supports the applicability of this instrument in cyberspace.[409]

However, the application of this instrument cannot ignore the risks associated with its misuse, and therefore it is necessary to insist on strict compliance with the conditions of its application, which stem from international law, and at the same time unequivocally reject any consideration of the possibility of using force to any extent that would be justified by this instrument.

The third instrument analysed were countermeasures. This circumstance precluding wrongfulness allows the injured state a truly effective defence, as it permits the interference with almost all rights of the target state to a relatively large extent, but the prerequisite for the implementation of countermeasures is the legal attribution of the malign cyber operations to the target state, which can be highly problematic in the context of cyber operations. Despite this fact, and despite the additional substantive and procedural conditions that must be met, countermeasures are an essential part of the repertoire of legal instruments that play an important role in the defence against cyber operations.

Within the relevant chapter, the issue of the application of countermeasures in cyberspace was analysed. Apart from attribution, the proportionality requirement of countermeasures can also be problematic with respect to the limited predictability of their consequences. A feature of countermeasures against cyber operations is the relatively widely supported retreat from the prior notifications of the responsible state that is commonly applied in other areas.

Attention has also been paid to three contentious issues related to countermeasures: the due diligence principle, forcible countermeasures and collective countermeasures. It can be concluded that the violation of the due diligence principle by the target state opens the possibility of using countermeasures despite the absence of attribution for the cyber attack as such. Forcible countermeasures can be ruled out, as although the Tallinn Manual 2.0 theoretically admits this possibility, there is no single state that takes the same view. Conversely, twelve states, including the US and Russia, have explicitly ruled out this possibility entirely. The possibility of collective countermeasures remains controversial, but there is growing support for the concept among states, which may prospectively lead to the establishment of this rule in general international law, at least in relation to cyberspace.

---

[409] CZECH REPUBLIC, MINISTRY OF FOREIGN AFFAIRS. Position paper on the application of international law in cyberspace [online]. Mzv.gov.cz. February 2024 [viewed 14 May 2024]. Available at: https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf.

The issue of the application of international law in cyberspace still offers several challenges - for example, defining the boundary between permissible retorsion measures against the infrastructure of a target state and impermissible interference with the sovereignty of that state or the question of the permissibility of collective countermeasures. At the same time, as state practice expands, whether in the form of official statements or actual cyber operations, there is a growing body of relevant information on which to address these issues in turn. Research in this area must therefore continue, as the clearer the rules governing state behavior in cyberspace are, the less likely there will be unintended escalation or other fatal consequences for the international community, states, and individuals.

List of sources

1. ABRAMS, A. Here's What We Know So Far About Russia's 2016 Meddling [online]. 18 April 2019 [viewed 23 February 2023]. Available from: https://time.com/5565991/russia-influence-2016-election/.
2. ANDERSON, T. Fitting a Virtual Peg into a Round Hole: Why Existing International Law Fails to Govern Cyber Reprisals. *Arizona Journal of International & Comparative Law*, 2016, 34(1).
3. ARIMATSU, L. and SCHMITT, M., N. The Plea of Necessity: An Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 2021, 97(1).
4. BANNELIER, K. and CHRISTAKIS, T. *Cyber-Attacks: Preventions-Reactions: The Role of States and Private Actors*. 1st ed. Paris: Les Cahiers de la Revue Défense Nationale, 2017.
5. BARNES, E. J. U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections. *nytimes.com* [online]. 23 October 2018 [viewed 23 February 2023]. Available from: https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html.
6. BBC. US imposes new Russia sanctions over cyber-attacks. *bbc.com* [online]. 11 June 2018 [viewed 23 February 2023]. Available from: https://www.bbc.com/news/world-us-canada-44446449.
7. BRAVERMAN, S. International Law in Future Frontiers: The Attorney General, the Rt Hon Suella Braverman QC MP, this evening set out in more detail the UK's position on applying international law to cyberspace. *gov.uk* [online]. 19 May 2022 [viewed 24 February 2023]. Available from: https://www.gov.uk/government/speeches/international-law-in-future-frontiers.
8. CARTOON NETWORK STUDIOS. *Rick and Morty: The Rickshank Rickdemption*. Burbank, USA: Cartoon Network Studios, 2017 [online]. [viewed 14 May 2024] Available from: https://www.youtube.com/watch?v=mweTc7tDO3I&ab_channel=AlephNull.
9. *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, ICJ, Judgement, 27 June 1986.
10. *Case Concerning The Gabčíkovo-Nagymaros Project (Hungary v. Slovakia)*, ICJ, Judgement, 25 September 1997.
11. CENTER FOR STRATEGIC & INTERNATIONAL STUDIES. *Significant cyber incidents*. [online] Washington, D. C.: CSIS [viewed 3 January 2022]. Available from: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
12. Charter of the United Nations from 1945.

13. CHESNEY, R. The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes. *lawfareblog.com* [online]. 25 September 2018 [viewed 19 February 2023]. Available from: https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes.

14. Convention on the Prevention and Punishment of the Crime of Genocide from 1948.

15. *Corfu Channel Case (UK v Albania)*, ICJ, Judgement, 9 April 1949.

16. COUNCIL OF THE EUROPEAN UNION. Council Conclusions On A Framework For A Joint EU Diplomatic Response To Malicious Cyber Activities ("Cyber Diplomacy Toolbox") of 19 June 2017. Available from: https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf.

17. COUNCIL OF THE EUROPEAN UNION. Council Decision 2019/797 of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States; Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

18. COUNCIL OF THE EUROPEAN UNION. Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities of 9 October 2017, p. 10. Available from: https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf.

19. COUNCIL OF THE EUROPEAN UNION. *EU Imposes the First Ever Sanctions against Cyber-Attacks* [viewed 3 January 2022]. Available from: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

20. CRAIG, A., VALERIANO, B. Conceptualising Cyber Arms Races. In: PISSANIDIS, N., RÕIGAS, H., VEENENDAAL (eds.). *2026 8th International Conference on Cyber Conflict*. Tallinn: NATO CCDCOE Publications, 2016, p. 141 – 158.

21. CYBER TOOLKIT. National positions. Cyberlaw.ccdcoe.org [online]. [viewed 14 May 2024]. Available from: https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions.

22. CYBER TOOLKIT. Scenario 06: Cyber countermeasures against an enabling State. Cyberlaw.ccdcoe.org [online]. [viewed 22 October 2023]. Available from: https://cyberlaw.ccdcoe.org/wiki/Scenario_06:_Cyber_countermeasures_against_an_enabling_State.

23. CZECH REPUBLIC, *Position paper on the application of international law in cyberspace*. [online] [viewed 14 May 2024], p. 16. Available from: https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf.

24. DAWIDOWICZ, M. Third-Party Countermeasures in International Law. 1st ed. New York: Cambridge University Press, 2017.

25. DELERUE, F. *Cyber operations and international law*. 1st ed. Cambridge: Cambdrige University Press, 2020.

26. DEPARTMENT OF THE PRIME MINISTER AND CABINET, NEW ZEALAND. *The Application of International Law to State Activity in Cyberspace*. [online]. Available from: https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf.

27. Dohnalová, A. and Bartoníček, R. Ukrajinských hrdinů. Praha přejmenovala část ulice Korunovační u ruské ambasády. *aktualne.cz* [online]. 22 April 2022 [viewed 23 February 2023]. Available from: https://zpravy.aktualne.cz/regiony/praha/ukrajinskych-hrdinu-praha/r~92302b02c21411ec8a24ac1f6b220ee8/.

28. EGAN, B. J. International Law and Stability in Cyberspace. *justsecurity.org* [online]. 10 November 2016 [viewed 23 February 2023]. Available from: https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf.

29. European Convention on Human Rights from 1950.

30. EUROPEAN PARLIAMENTARY RESEARCH SERVICE. *Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence* [online]. May 2020 [viewed 20 February 2023], p. 2. Available from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI(2020)651937_EN.pdf.

31. EUROPEAN UNION EXTERNAL ACTION. EU imposes first ever cyber sanctions to protect itself from cyber-attacks. *eeas.europa.eu* [online]. 30 July 2020 [viewed 23 February 2023]. Available from: https://www.eeas.europa.eu/eeas/eu-imposes-first-ever-cyber-sanctions-protect-itself-cyber-attacks_en.

32. FEDERAL DEPARTMENT OF FOREIGN AFFAIRS OF SWITZERLAND. *Switzerland's position paper on the application of international law in cyberspace*. [online]. Available from:

https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf.

33. FOREIGN, COMMONWEALTH AND DEVELOPMENT OFFICE OF THE UNITED KINGDOM. *Application of international law to states' conduct in cyberspace: UK statement.* [online] Available from: https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.

34. GEISS, R. and LAHMANN, H. Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention. In: ZIOLKOWSKI, K. (ed). *Peacetime Regime for State Activities in Cyberspace.* Tallinn: NATO CCD COE, 2013.

35. GIEGERICH, T. Retorsion. In: WOLFRUM, R. (ed.) *Max Planc Encyclopedia of Public International Law.* Oxford: OUP, 2017; BANKS, C. W. The Bumpy Road to a Meaningful International Law of Cyber Attribution. *AJIL Unbound*, 2019, 113(1).

36. GOVERNMENT OF CANADA. International Law applicable in cyberspace, international.gc.ca [online]. [viewed 22 October 2023]. Avaiable from: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a9.

37. GOVERNMENT OF THE KINGDOM OF THE NETHERLANDS. *Appendix: International law in cyberspace.* [online]. Available from: https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf.

38. GOVERNMENT OF THE UNITED KINGDOM. Cyber and International Law in the 21st Century. Gov.uk [online]. 23 May 2018 [viewed 3 November 2023]. Avaiable from: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

39. GOVERNMENT OFFICES OF SWEDEN. Position Paper on the Application of International Law in Cyberspace. *Regeringen.se* [online]. July 2022 [viewed 3 November 2023]. Available from: https://www.regeringen.se/4a1ce0/contentassets/2bf3882c23bb4fdfb935310b03d562a1/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf.

40. GRANT, J., P., BARKER, C., J. *Parry & Grant encyclopaedic dictionary of international law.* 3rd ed. New York: Oxford University Press, 2009.

41. HAATAJA, S. *Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics*. 1st ed. Oxfordshire: Routledge, 2020.

42. HINKLE, K., C. Countermeasures in the cyber context: One more thing to worry about. *Yale Journal of International Law*, 2011, 37(Fall).

43. INTERNATIONAL LAW COMMISSION. *Yearbook of the International Law Commission: Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*. 2001, vol. II, part two.

44. INTERNATIONAL LAW COMMISSION. *Yearbook of the International Law Commission: Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, 1980, vol. II, part two.

45. ITALY. *Italian Position Paper on `International Law and Cyberspace`*. Esteri.it [online]. [viewed 3 November 2023]. Available from: https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf.

46. JIBILIAN, I. and CANALES, K. The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal. *businessinsider.com* [online]. 15 April 2021 [viewed 23 February 2023]. Available from: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

47. KEMP, S. Digital 2024: Global Overview Report. *Datareportal.com* [online]. 31 January 2024 [viewed 14 May 2024]. Available from: https://datareportal.com/reports/digital-2024-global-overview-report.

48. KOSSEFF, J. Retorsion as a Response to Ongoing Malign Cyberoperations. In: JANČÁRKOVÁ, T., LINDSTRÖM, L., SIGNORETTI, M., TOLGA, I., VISKY, G. (eds.). *2020 12th International Conference on Cyber Conflict*. Tallinn: NATO CCDCOE Publications, 2020.

49. LAHMANN, H. *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution*. 1st ed. Cambridge: Cambridge University Press, 2020, pp. 201-257.

50. *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, ICJ, Advisory Opinion, 9 July 2004.

51. LOTRIONTE, C. Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law. *The Cyber Defense Review*, 2018, 3(2).

52. McDONALD, N. and McLEOD, A. 'Antisocial Behaviour, Unfriendly Relations': Assessing the Contemporary Value of the Categories of Unfriendly Acts and Retorsion in International Law. *Journal of Conflict & Security Law*, 2021, 26(2).

53. MINISTRY OF DEFENCE OF FRANCE. *International Law Applied to Operations in Cyberspace.* [online] [viewed 5 January 2022], p. 8. Available from: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

54. MINISTRY OF FOREIGN AFFAIR OF FINLAND: International law and cyberspace: Finland's national positions. Um.fi [online] [viewed 23 October 2023]. Available from: https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727.

55. MINISTRY OF FOREIGN AFFAIRS OF JAPAN. *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations.* [online] [viewed 5 January 2022], p. 5. Available from: https://www.mofa.go.jp/files/100200935.pdf.

56. MINISTRY OF FOREIGN AFFAIRS OF POLAND. The Republic of Poland's position on the application of international law in cyberspace. Gov.pl [online]. 29 December 2022 [viewed 4 November 2023]. Available from: https://www.gov.pl/attachment/3203b18b-a83f-4b92-8da2-fa0e3b449131.

57. MIRON, A. and TZANAKOPOULOS, A. Unilateral Coercive Measures and International Law. *The Left in the European Parliament*, 2022, 1(1).

58. MORELLO, C. and NAKASHIMA, E. U.S. imposes sanctions on North Korean hackers accused in Sony attack, dozens of other incidents. *washingtonpost.com* [online]. 13 September 2019 [viewed 23 February 2023]. Available from: https://www.washingtonpost.com/national-security/us-sanctions-north-korean-hackers-accused-in-sony-attack-dozens-of-other-incidents/2019/09/13/ac6b0070-d633-11e9-9610-fb56c5522e1c_story.html.

59. MORET, E. and PAWLAK, P. The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime? *iss.europa.eu* [online]. 12 July 2017 [viewed 23 February 2023], p. 2. Available from: https://www.iss.europa.eu/content/eu-cyber-diplomacy-toolbox-towards-cyber-sanctions-regime.

60. MORGAN, S. Top 10 Cybersecurity Predictions And Statistics For 2024. *Cybersecurityventures*.com [online]. 5 February 2024 [viewed 14 May 2024] Available from:

https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/.

61. NATO. Men in black - NATO's cybermen. *Nato.int* [online]. 24 April 2015 [viewed 4 November 2023]. Available from: https://www.nato.int/cps/en/natohq/news_118855.htm.

62. OHLIN, J., D. and MAY, L. *Necessity in International Law*. 1st ed. New York: Oxford University Press, 2016.

63. *Oil Platforms (Islamic Republic of Iran v. United States of America)*, ICJ, Judgement, 12 December 1996, separate opinon of Judge Simma.

64. OSULA, A., KASPER, A. and KAJANDER, A. EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 2022, 16(1).

65. ROGUSKI, P. *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*. The Hague Program For Cyber Norms Policy Brief. 2020, p. 18. Available from: https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/153989/roguski_application_of_international_law_to_cyber_operations_2020.pdf?sequence=1&isAllowed=y.

66. Rome Statute of the International Criminal Court from 1998.

67. ROSCINI, M. *Cyber Operations and the Use of Force in International Law*. 1st ed. New York: Oxford University Press, 2016.

68. RUYS, T. Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework. In: Herik, L. (ed.) *Research Handbook on UN Sanctions and International Law*. Cheltenham: Edward Elgar Publishing, 2017.

69. SANGER, D. E. Obama Strikes Back at Russia for Election Hacking. *nytimes.com* [online]. 29 December 2016 [viewed 23 February 2023]. Available from: https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html.

70. SCHALLER, C. Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*, 2017, 95 (1).

71. SCHMIDT, J. The Legality of Unilateral Extra-territorial Sanctions under International Law. *Journal of Conflict & Security Law*, 2022, 27(1).

72. SCHMITT N. M. "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law. *Virginia Journal of International Law*, 2015, 54(1).

73. SCHMITT, M. N. Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum. *Harvard National Security Journal*, 2017, 8 (2).

74. SCHMITT, M. N. The Sixth United Nations GGE and International Law in Cyberspace. *Justsecurity.org* [online]. 10 June 2021 [viewed 20 October 2023]. Available from: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.

75. SCHMITT, M. Top Expert Backgrounder: Russia's SolarWinds Operation and International Law. [online] New York: Just Security [viewed 5 January 2022]. Available from: https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.

76. SCHMITT, M., N. and WATTS, S. Beyond State-Centrism: International Law and Non-State Actors in Cyberspace. *Journal of Conflict & Security Law*, 2016, 21(3).

77. SCHMITT, M., N. and WATTS, S. Collective Cyber Countermeasures?. *Harvard National Securitys Journal*, 2021, 12(1).

78. SCHMITT, M., N. et al. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. 1st ed. Cambridge: Cambridge University Press, 2013.

79. SCHMITT, M., N. Expert Backgrounder: NATO Response Options to Potential Russia Cyber Attack. *Justsecurity.org* [online]. 24 February 2022 [viewed 4 November 2023]. Available from: https://www.justsecurity.org/80347/expert-backgrounder-nato-response-options-to-potential-russia-cyber-attacks/.

80. SCHMITT, M., N. Terminological Precision and International Cyber Law. *Lieber.westpoint.edu* [online]. 29 July 2021 [viewed 3 November 2023]. Available from: https://lieber.westpoint.edu/terminological-precision-international-cyber-law/.

81. SCHMITT, Michael, N. et al. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, 2017.

82. SCHÖNDORF, R. Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations. *International Law* Studies, 2021, 97(1).

83. SCHWEIGHOFER, E., BRUNNER, I. AND ZANOL, J. Malicious Cyber Operations, "Hackbacks" and International Law: An Austrian Example As a Basis for Discussion on Permissible Responses. *Masaryk University Journal of Law and Technology*, 2020, 14 (2).

84. SIMMONS, N. A Brave New World: Applying the International Law of War to Cyber-Attacks. *Journal of Law & Cyber Warfare*, 2014, 4(1).

85. SPÁČIL, J. Animus Aggressionis: The Role Of Intent in the Analysis of Armed Attack in Cyberspace. *Czech Yearbook of Public & Private International Law*, 2022, 13(1).

86. SPÁČIL, J. Attribution of Cyber Operations: Technical, Legal and Political Perspectives. *International and Comparative Law Review*, 2024, 24 (1) (to be published 2Q 2024).

87. SPÁČIL, J. Cyber Operations against Critical Financial Infrastructure: a Non-Destructive Armed Attack?. *International and Comparative Law Review*, 2022, 22(2).

88. SPÁČIL, J. Plea of Necessity: Legal Key to Protection against Unattributable Cyber Operations. *Masaryk University Journal of Law and Technology*, 2022, 16(2).

89. THE FEDERAL GOVERNMENT OF GERMANY. *On the Application of International Law in Cyberspace.* [online]. Available from: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.

90. The NATO Cooperative Cyber Defence Centre of Excellence. *CCDCOE to Host the Tallinn Manual 3.0 Process* [online]. Ccdcoe.org [viewed 12 February 2023]. Available from https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/.

91. THE NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE. European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox. *ccdcoe.org* [online]. [viewed 23 February 2023]. Available from: https://ccdcoe.org/incyder-articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/.

92. THE WHITE HOUSE. *Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment [online]*. 29 December 2016 [viewed 23 February 2023]. Available from: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and.

93. TIIRMAA-KLAAR, H. The Evolution of the UN Group of Governmental Experts on Cyber Issues. *Cyberstability Paper Series: New Conditions and Constellations in Cyber* [online]. December 2021 [viewed 14 May 2024]. Available at: https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf.

94. U. S. DEPARTMENT OF STATE. Holding Russia To Account. *state.gov* [online]. 15 April 2021 [viewed 23 February 2023]. Available from: https://www.state.gov/holding-russia-to-account/.

95. U.S. DEPARTMENT OF THE TREASURY: Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups. *treasury.com* [online]. 13 September 2019 [viewed 23 February 2023]. Available from: https://home.treasury.gov/news/press-releases/sm0312.

96. U.S. DEPARTMENT OF THE TREASURY. Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks. *treasury.com* [online]. 15 March 2018 [viewed 23 February 2023]. Available from: https://home.treasury.gov/news/press-releases/sm0312.

97. UN General Assembly Resolution 2625 from 24 October 1970 *("The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States").*

98. UN Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security n. A/176/135 of 14 July 2021.

99. UN Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security n. A/70/174 of 22 July 2015.

100. United Nations Security Council, Resolution 1368 (2001) adopted on 12 September 2001.

101. United Nations Security Council, Resolution 1373 (2001) adopted on 28 September 2001.

102. UNITED NATIONS. Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266 of 13 July 2021, UN Doc. A/76/136 [online] p. 30. [viewed 24 February 2023] Available from: https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf.

103. UNITED NATIONS. *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report.* [online]. Doc. A/AC.290/2021/CRP.2, 10 March 2021 [viewed 7 January 2022]. Available from: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

104. UNITED NATIONS. *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Chair's Summary.* [online]. Doc. A/AC.290/2021/CRP.3, 10 March 2021 [viewed 7 January 2022]. Available from: https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

105. UNITED NATIONS. *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.* [online]. Doc. A/68/98, 24 June 2013

[viewed 14 May 2024]. Available from: https://documents.un.org/doc/undoc/gen/n13/371/66/pdf/n1337166.pdf.

106. UNITED NATIONS. *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. [online]. Doc. A/76/135, 14 July 2021 [viewed 8 January 2022]. Available from: https://www.undocs.org/pdf?symbol=en/A/76/135.

107. VALUCH, J and HAMUĽÁK, O. Use of Force in Cyberspace. *International and Comparative Law Review*, 2020, 20 (2).

108. VIDMAR, J. The Use of Force as a Plea of Necessity. *American Journal of International Law Unbound*, 2017, 111.

109. von HEINEGG, Wolff Heintschel. Territorial Sovereignty and Neutrality in Cyberspace. *International Law Studies*, 2013, vol. 89.

110. WALLACE, D. and VISGER, M. The Use of Weaponized "Honeypots" under the Customary International Law of State Responsibility. *Cyber Defense Review*, 2018, 3(2).

Abstract

The subject of this paper is an analysis of three instruments of international law and their use in the context of cyber operations - retorsion, plea of necessity and countermeasures. These are legal instruments that can serve to legitimise defensive and retaliatory measures in response to cyber operations that might otherwise constitute violations of international law. The main aim of this paper is to analyse the possible uses of these instruments in the context of cyber operations, taking into account recent state practice (2019-2024), and to explore problematic aspects of their application, such as the possibility of the use of force or collective action.

Abstrakt

Předmětem této práce je analýza tří instrumentů mezinárodního práva a jejich použití v kontextu kybernetických operací – retorsion, plea of necessity and countermeasures. Jedná se o právní nástroje, jež mohou sloužit k legitimizaci obranných a odvetných opatření v reakci na kybernetické operace, jež by jinak mohly představovat porušení mezinárodního práva. Cílem této práce je především analyzovat možnosti použití těchto instruments v kontextu kybernetických operací při zohlednění recentní státní praxe (2019 – 2024) a prozkoumat problematické aspekty jejich aplikace, jako je např. možnost užití síly či kolektivní akce.

Key-words

retorstion, plea of necessity, countermeasures, cyber operations, international law

Klíčová slova

retorze, stav nouze, protiopatření, kybernetické operace, mezinárodní parvo veřejné