BALTIC JOURNAL OF LAW & POLITICS
A Journal of Vytautas Magnus University
VOLUME 117, NUMBER 1 (2024)
ISSN 2029-0454

Cit.: *Baltic Journal of Law & Politics* 17:1 (2024): 46–69
https://content.sciendo.com/view/journals/bjlp/bjlp-overview.xml
DOI: 10.2478/bjlp-2024-0003

RETORSION: AN UNDERRATED RETALIATORY MEASURE AGAINST MALIGN CYBER OPERATIONS

Jakub Spáčil

PhD Candidate
Palacký University Olomouc, Czech Republic

Contact information
Address: Tř. 17. listopadu 8, 771 11 Olomouc, Czech Republic
E-mail: jakubspacil@gmail.com
Phone: +420 774 922 806

Received: Septemer 4, 2023; reviews: 2; accepted: February 19, 2024.

ABSTRACT

The articles discusses the application of the concept of retorsion in relation to defensive measures against hostile cyber operations. Retorsion is a concept not regulated by international law, which gives the victim state a high degree of flexibility in its use. However, its limits are formed by the rules of international law (retorsion is an unfriendly act not prohibited by international law). The paper is divided into three main parts. The first part discusses the concept of retorsion in general terms and its relation to cyber operations, the second part defines the relationship between retorsion, countermeasures, plea of necessity and the right of self-defence, and the third part consists of in-depth analysis of states' practice. The analysis of states' practices includes both the actual measures that states have taken in response to cyber operations (e.g. expulsion of diplomats, economic sanctions, travel bans) and official statements on the issue that have been published, particularly in the period 2019–2022. Attention is also paid to the possibilities of using retorsion against cyber operations carried out by non-state actors.

KEYWORDS

Retorsion, cyber operations, cyber-attack, retaliatory measures, state responsibility.

INTRODUCTION[1]

When historians describe the second decade of the twenty-first 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.[2] 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[3] 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.[4]

As noted, retorsion is a concept that remains on the fringes of interest to international legal scholars. This fact had to be reflected in the chosen research methodology. Thus, the rigorous literature review resulted in a number of secondary sources published mainly in the period 2015–2020 and which therefore do not reflect the practice of states regarding cyber retorsion measures which has significantly expanded in the follow-up period 2019–2023. One of the main contributions of this article is precisely the mapping of the relevant practice of states in this period and drawing relevant conclusions.

The fundamental question of this paper is what role retorsion plays among other unilateral retaliatory remedies to cyber operations and what specific measures fall into this category and which do not. These questions are answered 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. 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

[1] This work was supported by a student project: "International legal aspects of defense against cyber operations: retorsion and countermeasures" (IGA_PF_2022_004) of the Palacký University. The article was supervised by prof. JUDr. Dalibor Jílek, CSc.

[2] Wolff Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace," *International Law Studies* 89 (2013): 123.

[3] Jeff Kosseff, "Retorsion as a Response to Ongoing Malign Cyberoperations": 15; in: T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, G. Visky, eds., *2020 12th International Conference on Cyber Conflict* (Tallinn: NATO CCDCOE Publications, 2020); Neil McDonald and Anna McLeod, "Antisocial Behaviour, Unfriendly Relations: Assessing the Contemporary Value of the Categories of Unfriendly Acts and Retorsion in International Law," *Journal of Conflict & Security Law* 26 (2021): 423.

[4] Martin Dawidowicz, *Third-Party Countermeasures in International Law* (New York: Cambridge University Press, 2017), 29.

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.[5] While the latter three concepts constitute so-called circumstances precluding wrongfulness,[6] the nature of retorsion is different.

Retorsion is "unfriendly conduct which is not inconsistent with any international obligation of the state engaging in it".[7] Typical examples of retorsion include protests, denial of access to state resources, economic sanctions or expulsion of diplomats.[8] 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.[9] 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.[10] 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.[11]

Retorsion is not a right. Rather, it should be referred to as freedom.[12] As a result, it is not a legal concept, but a descriptive category (or technical term),[13] which has no direct legal effect.[14] Freedom, unlike right, is not limited by conditions.[15] 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 an 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),[16] and on the other hand by international law, because although retorsion itself is not regulated by international law,[17] it is the rules of international law that constitute its limit.[18] 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),

---

5 Michael N. Schmitt et al., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 82.

6 International Law Commission, *Yearbook of the International Law Commission: Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries,* Vol. II, part two (2001): 71–86 (hereinafter also ARSIWA).

7 *Ibid.*, 128.

8 Thomas Giegerich, "Retorsion": in: Rüdiger Wolfrum, ed., *Max Planc Encyclopedia of Public International Law* (Oxford: OUP, 2017); William C. Banks, "The Bumpy Road to a Meaningful International Law of Cyber Attribution," *AJIL Unbound* 113 (2019): 194.

9 Neil McDonald and Anna McLeod, *supra* note 3*,* 425.

10 *Ibid.*

11 *Ibid.*, 421; Tom Ruys, "Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework": 24; in: Larissa van den Herik, ed., *Research Handbook on UN Sanctions and International Law* (Cheltenham: Edward Elgar Publishing, 2017); International Law Commission, *supra* note 6, 128.

12 Tom Ruys, *supra* note 11, 24; Martin Dawidowicz, *supra* note 4, 28.

13 John P. Grant and Craig J. Barker, *Parry & Grant encyclopaedic dictionary of international law* (New York: Oxford University Press, 2009), 525.

14 Neil McDonald and Anna McLeod, *supra* note 3*,* 424.

15 Tom Ruys, *supra* note 11, 24.

16 Jeff Kosseff, *supra* note 3, 15.

17 Martin Dawidowicz, *supra* note 4, 28.

18 Neil McDonald and Anna McLeod, *supra* note 3*,* 441.

and if a state violates a rule of international law by its conduct, such conduct (or omission) cannot be described as retorsion.[19] 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.[20]

Retorsion should be distinguished from an "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.[21] However, for both categories it is true that they are lawful measures.[22]

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.[23] Nor is the State limited in relation to the motive, purpose, duration or character of the measure chosen.[24] Retorsion may thus justify even measures constituting mere revenge.[25] The question of whether retorsion is justified is not a matter for legal consideration at all.[26] The fact remains that, despite the absence of regulation, states tend to use proportionate measures in order to pursue "just and sound politics".[27] The question is whether, in the case of wholly malicious hostile conduct, this could be an abuse of the law, as Giegerich suggests.[28] The fact is that such conduct would be contrary to the requirement of friendly relations among states.[29] 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.[30] 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.[31]

If retorsion is not regulated by law, does it make sense to address it from a legal perspective? It undoubtedly does, 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.[32] 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

---

19 Jeff Kosseff, *supra* note 3, 15.
20 *Ibid.*, 11.
21 Neil McDonald and Anna McLeod, *supra* note 3*,* 427.
22 *Ibid.,* 422.
23 *Ibid.,* 424; Tom Ruys, *supra* note 11, 24; Martin Dawidowicz, *supra* note 4, 28.
24 Jeff Kosseff, *supra* note 3, 15–16; Martin Dawidowicz, *supra* note 4, 28.
25 Michael N. Schmitt et al., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 40.
26 Troy Anderson, "Fitting a Virtual Peg into a Round Hole: Why Existing International Law Fails to Govern Cyber Reprisals," *Arizona Journal of International & Comparative Law* 34 (2016): 144; John P. Grant and Craig J. Barker, *supra* note 13, 525; Martin Dawidowicz, *supra* note 4, 28.
27 Martin Dawidowicz, *supra* note 4, 28.
28 Thomas Giegerich, *supra* note 8; Julia Schmidt, "The Legality of Unilateral Extra-territorial Sanctions under International Law," *Journal of Conflict & Security Law* 27 *(*2022): 73.
29 UN General Assembly Resolution 2625 from 24 October 1970 *("The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States")*.
30 Jeff Kosseff, *supra* note 3, 16.
31 Julia Schmidt, *supra* note 28, 73; Neil McDonald and Anna McLeod, *supra* note 3*,* 424.
32 Neil McDonald and Anna McLeod, *supra* note 3*,* 424.

signals to the state concerned that it is acting within the bounds of international law, which can have a de-escalatory effect.[33]

The use of the concept of retorsion has 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 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.[34] However, there are risks – the main one being the potential misuse of the concept to illegitimately justify internationally wrongful conduct.[35]

With reference to the work of White and Abass, Ruys states that "the issue of enforcement by means of non-forcible measures is and remains 'one of the least developer areas of international law'".[36] This conclusion 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,[37] 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"[38] on the application of international law in cyberspace, contains only six brief mentions of retorsion (although, for example, countermeasures is the subject of six rules elaborated over 20 pages).[39] One can only hope that the third edition of the Tallinn Manual will already give sufficient attention to this issue.[40]

2. RETORSION VS. OTHER UNILATERAL REMEDIES

Under the concept of retorsion, one can include such actions of the state that are a priori legal regardless of the circumstances. Every state is entitled to implement retorsion measures at any time and without limitation.[41] However, they are usually relatively ineffective measures.[42] If we rank the concepts of international law that can be used to justify retaliatory measures against a cyber operation on the basis of their effectiveness, then generally the least effective will be retorsion, slightly higher effectiveness is provided by countermeasures and plea of necessity (which are comparably effective among themselves) and the highest coercive potential can be expected from the right of self-defence, which is associated with the possibility of the use of force. The latter three concepts, however, can be combined with retorsion, and it is this relationship that is the focus of the next section.

---

33 *Ibid.*
34 Neil McDonald and Anna McLeod, *supra* note 3*,* 435–438.
35 *Ibid.,* 440.
36 Tom Ruys, *supra* note 11, 23.
37 Neil McDonald and Anna McLeod, *supra* note 3*,* 433.
38 European Parliamentary Research Service, *Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence,* (May 2020) // https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI(2020)651937_EN.pdf
39 Michael N. Schmitt et al., *supra* note 5, 112, 118, 131.
40 The NATO Cooperative Cyber Defence Centre of Excellence, *CCDCOE to Host the Tallinn Manual 3.0 Process* // https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/
41 Catherine Lotrionte, "Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law," *The Cyber Defense Review* 3 (2018): 92.
42 Troy Anderson, *supra* note 26, 145.

2.1. Retorsion and Countermeasures

The essential difference between retorsions and countermeasures is that while actions falling under the concept of retorsions are always legal, countermeasures are those actions of a state that constitute a violation of international law but whose illegality is precluded by the prior internationally wrongful act[43] of the state against which they are directed.[44]

Countermeasures, unlike retorsion, are a regulated legal instrument of international law.[45] Their use is thus limited by a number of conditions. Countermeasures can only be implemented against conduct attributable to a state.[46] However, to attribute a cyber operation poses a major challenge since it is often carried out via non-state actors and/or the direct connection to a state is covert.[47] Further, such conduct must constitute a violation of international law, but such a conclusion is not always easy to draw and a number of contentious situations arise.[48] An example of a contentious situation is the question of whether influence of electoral processes is a violation of the principle of non-intervention.[49] Countermeasures are also limited by the objective pursued, as they can only be implemented "to induce that state to comply with its obligations".[50] The temporal effect of countermeasures is also limited to the duration of the primary violation of international law by the state concerned.[51] Last but not least, countermeasures have to be proportional to "the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question".[52] There is also a procedural requirement of notification of the responsible state associated with the implementation of countermeasures, but this is a requirement that can significantly reduce the effectiveness of such countermeasures in the context of cyber operations.[53]

The question of the admissibility of collective countermeasures is also relevant. For the moment, it can be stated that although there are voices supporting collective countermeasures,[54] this idea is not supported by a broader international consensus.[55]

Countermeasures can be more effective than retorsion, as they allow for conduct that otherwise constitutes a violation of international law, but their real applicability in practice is significantly limited by a number of conditions, some of which (e.g. attribution) may be almost impossible to meet in the context of cyber operations. Therefore, one can fully agree with Jeff Kosseff, who concluded that states "should consider whether some responses can be classified as retorsion rather than countermeasure", as many measures intended as countermeasures can meet the definition of retorsion with minimal adaptation.[56] At the same time, care should be taken to ensure that states

---

43 Definition of internationally wrongful act is provided in art. 2 of International Law Commission, *supra* note 6 (ARSIWA): "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."

44 International Law Commission, *supra* note 6, 75–76.

45 *Ibid.*

46 *Ibid.*, 129.

47 Michael N. Schmitt, *Terminological Precision And International Cyber Law (*29 July 2021) // https://lieber.westpoint.edu/terminological-precision-international-cyber-law; Michael N. Schmitt et al., *supra* note 5, 87.

48 Jeff Kosseff, *supra* note 3, 11.

49 *Ibid.*

50 International Law Commission, *supra* note 6, 129.

51 *Ibid.*; Jeff Kosseff, *supra* note 3, 13.

52 International Law Commission, *supra* note 6, 134.

53 *Ibid.*, 135; Jeff Kosseff, *supra* note 3, 14.

54 Jeff Kosseff, *supra* note 3, 14.

55 *Ibid.*

56 *Ibid*.

clearly delineate whether they are acting on the basis of retorsion or countermeasures in a particular case, as incorrect categorization could lead to inappropriate and unnecessary application of limiting conditions on the one hand, and increase the risk of unintended escalation on the other.[57]

But there is perhaps an even more important connection between retorsion and countermeasures. Although collective countermeasures are not allowed by international law, nothing prevents the implementation of countermeasures by an aggrieved state with the simultaneous support of other states through measures at the level of retorsion, since retorsion, as always a legal action, is available even to states not directly harmed by a cyber operation.[58] Countermeasures and retorsions often occur simultaneously in practice already. [59]

2.2. Retorsion and the Plea of Necessity

Plea of necessity is another circumstance precluding wrongfulness.[60] It is an instrument of international law which, like countermeasures, is limited by a number of conditions, but which, if met, allows the implementation of an act that would otherwise be a violation of international law. The principal advantage of this instrument is the possibility for the injured state to implement protective measures against a territorial state (the state from whose territory the cyber operation originates) without having to prove that this state bears international legal responsibility for the cyber operation (i.e. without having to prove that the cyber operation is attributable to this state).[61]

Plea of necessity can be invoked only if the applied protective measure "is the only way for the State to safeguard an essential interest against a grave and imminent peril and 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".[62] Plea of necessity, like countermeasures, however, cannot justify measures that would violate the prohibition on the threat and use of force. [63]

Plea of necessity has an undeniable advantage over countermeasures in that it can be used even in the absence of attributability of the conduct to the territorial state. This advantage is, however, limited by extremely high requirements for the fulfilment of other conditions (protection of essential interest, existence of grave and imminent peril, etc.). If these conditions are met, the range of justifiable actions is similar to the measures that can be taken on the basis of countermeasures.

What is the role of retorsion in relation to the plea of necessity? Retorsion may be a suitable alternative to less invasive defensive measures when the conditions for the application of plea of necessity are not clearly met. At the same time, retorsion measures can be used by third states to support the position of an injured State acting on the basis of the plea of necessity.

---

57 Neil McDonald and Anna McLeod, *supra* note 3*,* 440.
58 Jeff Kosseff, *supra* note 3, 17; Michael N. Schmitt et al., *supra* note 5, 131.
59 Martin Dawidowicz, *supra* note 4, 29.
60 International Law Commission, *supra* note 6, 80.
61 International Law Commission, *supra* note 6, 80; Jakub Spáčil, "Plea of Necessity: Legal Key to Protection Against Unattributable Cyber Operations," *Masaryk University Journal of Law and Technology* 16 (2022): 218.
62 International Law Commission, *supra* note 6, 80.
63 Jakub Spáčil, *supra* note 61, 233.

2.3. Retorsion and Self-Defence

Even a cyber operation can fulfil the characteristics of an armed attack,[64] which activates the right of self-defence of the victim state.[65] Self-defence is an exception to the prohibition on the use of force.[66] International legal scholarship has addressed the topic of self-defence against cyber operations reaching the level of an armed attack very thoroughly in the last decade,[67] but in practice there has not yet been a single example of a state actually invoking the right of self-defence in response to a cyber operation.

It is therefore not necessary to deal with this institution in more depth at this point and it is sufficient to state that in relation to the right to self-defence the importance of retorsion is negligible. The right of self-defence also includes the possibility of requesting the assistance of third states (collective self-defence), and it is not necessary to look for other justifications for the assistance of third states, as is the case with countermeasures and the plea of necessity.[68] That does not mean, however, that retorsion could not also be used in such a situation. Nor can retorsion be considered as an alternative to the right of self-defence, since it cannot be used to legitimize the use of force in any case.[69]

Finally, measures taken on the basis of retorsion will usually be wholly disproportionate (inadequate) to the gravity of the violation of international law when a violation of the prohibition on the use of force is at stake. On the other hand, however, such a situation cannot be entirely ruled out. In 2019, a surveillance drone operated by the US Army over the Persian Gulf was shot down.[70] The Islamic Revolutionary Guard Corps was behind the attack.[71] In response to this event, the US initially planned a military airstrike against Iran, a use of force justified only by the right of self-defence, but in the end, in the interests of proportionality, the retaliation chosen was a cyber operation to disable a "crucial database used by Iran's elite paramilitary force to target oil tankers and shipping traffic".[72] This operation is probably closer to countermeasures than retorsion given the intrusion on Iran's sovereignty, but given the unclear position of the applicability of sovereignty in cyberspace[73] it can at least be classified in the "grey zone" and could theoretically be considered mere retorsion.

2.4. Partial Conclusion

In the previous section it was demonstrated that in many cases, retorsion can either be an alternative to other unilateral measures or can be used by third states to support these remedies. However, there is another important advantage to favoring retorsion

---

64 For a detailed analysis of approaches to "armed attack" in cyberspace see Jozef Valuch and Ondrej Hamuľák, "Use of Force in Cyberspace," *International and Comparative Law Review* 20 (2020): 174–191.
65 Charter of the United Nations, art. 51.
66 *Ibid.*, art. 4(2).
67 See e. g. Henning Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge: Cambridge University Press, 2020); Michael N. Schmitt, "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: an Analytical Vade Mecum," *Harvard National Security Journal* 8 (2017); or Michael N. Schmitt et al., *supra* note 5, 339–357.
68 Charter of the United Nations, art. 51: "…inherent right of individual or collective self-defence…"
69 Troy Anderson, *supra* note 26, 143.
70 Ellen Nakashima and Paul Sonne, *U.S. military carried out secret cyberstrike on Iran to prevent it from interfering with shipping* (28 August 2019) // https://www.washingtonpost.com/national-security/us-military-carried-out-secret-cyber-strike-on-iran-to-prevent-it-from-interfering-with-shipping/2019/08/28/36202a4e-c9db-11e9-a1fe-ca46e8d573c0_story.html
71 *Ibid.*
72 *Ibid.*
73 Jeff Kosseff, *supra* note 3, 12.

where possible. This advantage is crucial in situations where the injured state misidentifies the responsible state or misjudges the fulfilment of the prerequisites and conditions of the circumstance precluding wrongfulness. Retorsion is always lawful, even if there is a mistake as to the responsible state or if the defensive measure turns out to be inappropriate or disproportionate. In such a situation, while retorsion may take on more of an unfriendly act quality, it will never be an internationally wrongful act that could lead to further escalation. From this perspective it is thus preferable, if such a course of action is sufficiently effective, to prefer retorsion to other unilateral measures.

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. The next section is devoted to the analysis of these forms of state practice.

3.1. Application of Retorsion Measures

One of the first examples of a major state sponsored cyber operation is the cyber activity directed at Estonian banks and public services in 2007.[74] Among the measures taken by the affected institutions in cooperation with the government was blocking access to certain IP addresses from Russia.[75] 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.[76]

Russian intelligence services interfered in the 2016 US presidential election through, among other things, cyber operations.[77] 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.[78] The US responded to the election meddling with the expulsion of 35 Russian diplomats.[79] Expulsion of diplomats is a typical example of retorsion.[80] 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.[81] A series of additional sanctions, at least some of which could be considered retorsion, followed in 2018.[82]

---

74 Michael N. Schmitt et al., *supra* note 25, 40.
75 *Ibid.*
76 Michael N. Schmitt, "Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law," *Virginia Journal of International Law* 54 (2015): 701.
77 David E. Sanger, *Obama Strikes Back at Russia for Election Hacking,* (29 December 2016) // https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html
78 Abigail Abrams, *Here's What We Know So Far About Russia's 2016 Meddling*, (18 April 2019) // https://time.com/5565991/russia-influence-2016-election/
79 David E. Sanger, *supra* note 77; see also Troy Anderson, *supra* note 26, 142.
80 Neil McDonald and Anna McLeod, *supra* note 3*,* 422.
81 The White House, *Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment*, *(*29 December 2016) // https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and; see also Samuli Haataja, *Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics* (Oxfordshire: Routledge, 2020), 180–181.
82 BBC, *US imposes new Russia sanctions over cyber-attacks*, (11 June 2018) // https://www.bbc.com/news/world-us-canada-44446449; U.S. Department of the Treasury, *Treasury Sanctions Russian Cyber*

North Korea uses cyber operations mainly to raise funds, but also to protect its interests.[83] Therefore, in 2019, the US adopted sanctions against three groups linked to the North Korean government – Lazarus Group, Bluenoroff, and Andariel.[84] 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".[85] Again, these are measures not prohibited under international law, and thus a retorsion.[86]

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[87] managed to spy on private companies and US government agencies for several months via malicious code.[88] Spying is not an illegal act under international law,[89] 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, and sanctions also targeted individuals and companies associated with Russian cyber activities, and there were expulsions of several Russian officials from the US.[90]

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, in a case 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".[91] 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.[92] Nevertheless, its use 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).

Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks, (15 March 2018) // https://home.treasury.gov/news/press-releases/sm0312; Samuli Haataja, *supra* note 81, 181.

83 Carol Morello and Ellen Nakashima, *U.S. imposes sanctions on North Korean hackers accused in Sony attack, dozens of other incidents*, (13 September 2019) // 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

84 U.S. Department of the Treasury, *Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups*, (13 September 2019) // https://home.treasury.gov/news/press-releases/sm0312

85 *Ibid.*

86 Catherine Lotrionte, *supra* note 41, 92; Jeff Kosseff, *supra* note 3, 18.

87 Neil McDonald and Anna McLeod, *supra* note 3*,* 431.

88 Isabella Jibilian and Katie Canales, *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*, (15 April 2021) // https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

89 Michael N. Schmitt et al., *supra* note 5, 168.

90 Neil McDonald and Anna McLeod, *supra* note 3*,* 422, 431; U. S. Department of State, *Holding Russia To Account*, (15 April 2021) // https://www.state.gov/holding-russia-to-account/

91 European Union External Action, *EU imposes first ever cyber sanctions to protect itself from cyber-attacks,* (30 July 2020) // https://www.eeas.europa.eu/eeas/eu-imposes-first-ever-cyber-sanctions-protect-itself-cyber-attacks_en

92 Neil McDonald and Anna McLeod, *supra* note 3*,* 430.

Given the current geopolitical instability, mainly the Russian-Ukrainian war, it could be tempting to include cyber aspects of this conflict into this article. However, it is doubtful whether relevant conclusions could be drawn from the practice which emerged during an armed conflict. There is no doubt that cyber operations play an important role in the Russian-Ukrainian conflict.[93] It is also true that many of them would not in themselves constitute a violation of international law, and therefore could be assessed as acts of retorsion.[94] However, these cyber operations occur in the context of an armed conflict in which the attacked party (Ukraine) can justify any lesser intensive operation on the basis of the right to self-defence. In other words, no party to an armed conflict has a reason to invoke retorsion in a situation where there is another, more permissive circumstance precluding illegality, and therefore, one cannot even draw relevant conclusions from this practice for the application of retorsion measures, which, on the contrary, typically occur in outside of the context of armed conflicts.

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.

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*."[95] Other States have subsequently taken a similar view in their national positions, namely the Netherlands (2019),[96] New Zealand (2020),[97]

---

93 Stéphane Duguin, Pavlina Pavlova, *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*, *(*September 2023) // https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf

94 *Ibid*., p. 8.

95 Brian J. Egan, *International Law and Stability in Cyberspace*, (10 November 2016) // 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* // https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf

96 Government of the Kingdom of the Netherlands, *Appendix: International law in cyberspace //* 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

97 Department of the Prime Minister and Cabinet, New Zealand, *The Application of International Law to State Activity in Cyberspace* // https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf

Estonia (2021),[98] Germany (2021),[99] Norway (2021),[100] Singapore (2021),[101] Switzerland (2021)[102] and the United Kingdom (2022).[103]

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,[104] asset freezes,[105] travel bans,[106] economic or other measures against individuals and entities,[107] "limiting or cutting off the other state's access to servers or other digital infrastructure in its territory",[108] limiting or breaking off diplomatic relations,[109] imposing sanctions,[110] publicly attributing a cyber operation to another state,[111] refraining from signing a trade agreement,[112] recalling an ambassador,[113] restrictions on freedom of movement[114] and exclusion from international groupings.[115]

The importance of collective actions based on retorsion, which naturally achieve greater effectiveness, is also emphasized.[116] This is, after all, one of the basic principles also mentioned in the "cyber diplomacy toolbox" of the European Union.[117]

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.[118] 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.[119] This document set out the basic principles for

98 United Nations, *supra* note 93, 23–30.
99 The Federal Government of Germany, *On the Application of International Law in Cyberspace //* https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf
100 United Nations, *supra* note 93, 65–75.
101 United Nations, *supra* note 93, 83–85.
102 Federal Department of Foreign Affairs of Switzerland, *Switzerland's position paper on the application of international law in cyberspace //* https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf
103 Foreign, Commonwealth and Development Office of the United Kingdom, *Application of international law to states' conduct in cyberspace: UK statement //* 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
104 United Nations, *supra* note 93, 29.
105 *Ibid.*
106 *Ibid.*
107 Government of the Kingdom of the Netherlands, *supra* note 94.
108 *Ibid.*
109 United Nations, *supra* note 93, 72.
110 *Ibid.*
111 United Nations, *supra* note 93, 72.
112 Federal Department of Foreign Affairs of Switzerland, *supra* note 100.
113 *Ibid.*
114 Suella Braverman, *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*, (19 May 2022) // https://www.gov.uk/government/speeches/international-law-in-future-frontiers
115 *Ibid.*
116 Suella Braverman, *supra* note 112; United Nations, *supra* note 93, 28.
117 European Parliamentary Research Service, *supra* note 38, 9.
118 *Ibid.,* 1.
119 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* // https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf

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".[120] 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.[121] Its disclosure then also pursues the preventive goal of deterring a potential aggressor.[122] 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.[123]

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.[124] 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".[125] These measures may include, inter alia, "travel bans, arms embargoes, freezing funds or economic resources".[126] 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.[127] Other official EU documents even refer to collective action as necessary "for the response to be effective".[128] 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), 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

---

120 *Ibid.,* 4

121 The NATO Cooperative Cyber Defence Centre of Excellence, *European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox* // https://ccdcoe.org/incyder-articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/; European Parliamentary Research Service, *supra* note 38, 2; *see also* Erica Moret and Patryk Pawlak, *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime? (*12 July 2017) // https://www.iss.europa.eu/content/eu-cyber-diplomacy-toolbox-towards-cyber-sanctions-regime

122 European Parliamentary Research Service, *supra* note 38, 8.

123 *Ibid*., 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* // https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf

124 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.

125 Council of the European Union, *supra* note 121, 9.

126 *Ibid*.

127 *Ibid.*

128 European Parliamentary Research Service, *supra* note 38, 8.

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.

4. AVAILABLE RETORSION MEASURES

Retorsion is not a new concept that is unique to responses to cyber operations.[129] 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.

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.[130] As the literature and state practice 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,[131]
- withdrawing from an international organization,[132]
- recalling own ambassador,
- summoning a foreign ambassador,[133]
- restriction of movement,
- exclusion from international groupings,
- canceling bilateral visits,[134]
- denying access to ports,[135]
- boycott of the Olympic Games,[136]

[129] Neil McDonald and Anna McLeod, *supra* note 3*,* 443.
[130] Przemyslaw Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views //* https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/153989/roguski_application_of_international_law_to_cyber_operations_2020.pdf?sequence=1&isAllowed=y
[131] Neil McDonald and Anna McLeod, *supra* note 3*,* 427.
[132] *Ibid.*
[133] *Ibid.*
[134] *Ibid.*
[135] *Ibid.*
[136] *Ibid*.

- renaming of a place (e.g. street, square),[137]
- terminating cultural and educational exchanges,[138] and
- reduction of foreign aid.[139]

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.[140] Norway has also explicitly subsumed this practice under retorsion in its official national position.[141] 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.[142] Domestic indictment of entities and individuals from responsible states can play a similar role.[143] 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.[144]

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 obligations not provided for by general international law.[145] 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; however, each case must be considered on its own merits.[146]

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,[147] 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.[148]

---

137 Martin Dawidowicz, *supra* note 4, 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* Anna Dohnalová and Radek Bartoníček, *Ukrajinských hrdinů. Praha přejmenovala část ulice Korunovační u ruské ambasády*, (22 April 2022) // https://zpravy.aktualne.cz/regiony/praha/ukrajinskych-hrdinu-praha/r~92302b02c21411ec8a24ac1f6b220ee8/

138 Catherine Lotrionte, *supra* note 41, 92.

139 International Law Commission, *supra* note 6, 128.

140 Neil McDonald and Anna McLeod, *supra* note 3*,* 431.

141 United Nations, *supra* note 93, 72.

142 *Ibid.*

143 Jeff Kosseff, *supra* note 3, 17.

144 The White House, *supra* note 81; Samuli Haataja, *supra* note 81, 180–181.

145 Tom Ruys, *supra* note 11, 24; Michael N. Schmitt et al., *supra* note 5, 112.

146 Julia Schmidt, *supra* note 28, 71.

147 *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, International Court of Justice (Judgement of 27 June 1986), para. 244–245.

148 For a thorough discussion of the issue, see Tom Ruys, *supra* note 11, 24; see also Julia Schmidt, *supra* note 28, 71.

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.[149]

4.2.1. Limitation of Access to Cyber Infrastructure

States have full sovereignty over the cyber infrastructure located on their territory.[150] 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.[151] The only limit to this is any treaty obligations relating to cyber infrastructure.[152] Restriction of access was already implemented in practice by Estonia in 2007 when it banned access to certain IP addresses registered in Russia.[153] 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.[154]

4.2.2. 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.[155] 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 state's own 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."[156] 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. 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

149 Jeff Kosseff, *supra* note 3, 17–22.
150 Michael N. Schmitt et al., *supra* note 5, 13.
151 Michael N. Schmitt et al., *supra* note 5, 112.
152 Catherine Lotrionte, *supra* note 41, 92.
153 Michael N. Schmitt et al., *supra* note 25, 40.
154 Government of the Kingdom of the Netherlands, *supra* note 94.
155 Jeff Kosseff, *supra* note 3, 19.
156 Michael N. Schmitt et al., *supra* note 5, 565.

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".[157] Espionage is generally not prohibited by international law and is therefore nothing more than retorsion.[158] 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.[159]

4.2.3. Operations on or Against an Adversary's Cyber Infrastructure

Merely mapping an adversary's cyber infrastructure without manipulating the data is a form of espionage and as such is 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).[160]

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.[161] 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".[162] The crucial question is whether the transmission of the malicious code was carried out by the injured state of its own will (state B), and whether 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),[163] 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 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.[164] 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

157 Jeff Kosseff, *supra* note 3, 18.
158 Michael N. Schmitt et al., *supra* note 5, 168.
159 Michael N. Schmitt et al., *supra* note 5, 168; Jeff Kosseff, *supra* note 3, 19.
160 Jeff Kosseff, *supra* note 3, 21–22; Robert Chesney, *The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes*, (25 September 2018) // https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes
161 Jeff Kosseff, *supra* note 3, 20;
162 Michael N. Schmitt et al., *supra* note 5, 174.
163 *Ibid.*
164 *See* Jakub Spáčil, "Animus Aggressionis: The Role Of Intent in the Analysis of Armed Attack in Cyberspace," *Czech Yearbook of Public & Private International Law* 13 (2022): 58–59.

the fulfilment of the prerequisites of one of the circumstances precluding wrongfulness is required to justify them.[165]

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.[166]

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.[167] 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).[168] Such an interference does not meet the defining characteristics of retorsion and requires justification by another instrument of international law for its legality.

4.2.4. Warning of Individual Operatives

In some cases, states are able to identify the specific individuals conducting cyber operations.[169] 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 have identified them and are tracking their work".[170] 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".[171]

The conclusion as to whether the above practice can be considered 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.[172]

5. SIDE-NOTE: RETORSION AND NON-STATE ACTORS

Cyber operations are often carried out by non-state actors, whether acting of their own will or in cooperation with or at the command of a state. Non-state actors can include individual hackers, hacker groups or terrorist organizations. Proving that a particular state is responsible for the actions of these entities is often a significant problem.[173] If it is not possible to establish the international legal responsibility of another state, this

[165] David Wallace and Marc Visger, "The Use of Weaponized "Honeypots" under the Customary International Law of State Responsibility," *Cyber Defense Review* 3 (2018): 38.
[166] *Ibid.*, 33.
[167] Jeff Kosseff, *supra* note 3, 22.
[168] Michael N. Schmitt et al., *supra* note 5, 19.
[169] Jeff Kosseff, *supra* note 3, 17.
[170] Julian E. Barnes, *Begins First Cyberoperation Against Russia Aimed at Protecting Elections*, (23 October 2018) // https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html
[171] *Ibid.*
[172] Jeff Kosseff, *supra* note 3, 21.
[173] Michael N. Schmitt, *supra* note 47.

limits the legal defensive measures available to the attacked state. Countermeasures are excluded and the possibility of using self-defence is controversial to say the least.[174] De facto, in such a situation, the attacked state has no choice but to take a measure that falls under one of the remaining concepts of international law that allow for retaliatory action – retorsion or plea of necessity. Recourse to plea of necessity, however, is only possible under a number of strict conditions and thus often will not be available in practice.[175] Conversely, action based on retorsion is the only measure that is always available.

From the perspective of a state that has become the target of a cyber operation carried out by a non-state actor, two categories of retorsion measures will be relevant – retorsion directly against the attacking entity and retorsion against the state from whose territory the attack is conducted (territorial state). In the first case, it will typically be one of the cyber retorsion operations that produces a direct effect on the part of the attacker (e.g. denying access or warning a particular attacker of the possible consequences). In the second case, the aim of the attacked state will be to induce the territorial state to take measures in favor of the attacked state that the attacked state cannot implement itself, given the limits of international law (e.g. neutralizing the hostile cyber infrastructure or other law enforcement action). In this context, then, the violation of the principle of due diligence may also play a role, opening the possibility of taking more invasive measures as countermeasures.[176]

The fact is that retorsion will often be the only way to defend against cyber operations by non-state actors.

CONCLUSION

The articles aims 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, the relationship between retorsion and three legal concepts, the circumstances precluding wrongfulness – countermeasures, plea of necessity and self-defense – was discussed. Retorsion emerged as an important concept which, although not an instrument of international law, has its indispensable place in the adoption of retaliatory measures and their communication to the international community. Indeed, their designation as retorsion has an undeniable de-escalatory effect and clearly defines that the state considers its actions to be in conformity with international law. The fundamental advantage of retorsion over the other concepts mentioned is its accessibility, since it is available in virtually all circumstances and regardless of the responsibility of the state against which it is implemented. Conversely, its inherent disadvantage

[174] International Law Commission, *supra* note 6, 129; Michael N. Schmitt, "The Law of Cyber Warfare: Quo Vadis?" *Stanford Law and Policy Review* 25 (2014): 287; Michael N. Schmitt et al., *supra* note 5, 94.
[175] *See* Jakub Spáčil, *supra* note 61.
[176] Michael N. Schmitt et al., *supra* note 5, 30.

is its lower effectiveness, as the measures taken cannot affect the rights of other states and the range of available measures is thus significantly limited.

In the third 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 fourth part is 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.

In the fifth and las part, the importance of retorsion in relation to cyber operations carried out by non-state actors was briefly discussed.

In conclusion: 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 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.

BIBLIOGRAPHY

1. Abrams, Abigail. *Here's What We Know So Far About Russia's 2016 Meddling.* (18 April 2019) // https://time.com/5565991/russia-influence-2016-election
2. Anderson, Troy. "Fitting a Virtual Peg into a Round Hole: Why Existing International Law Fails to Govern Cyber Reprisals." *Arizona Journal of International & Comparative Law* 34 (2016): 144.
3. Banks, William C. "The Bumpy Road to a Meaningful International Law of Cyber Attribution." *AJIL Unbound* 113 (2019): 194.
4. Barnes, Julian E. *Begins First Cyberoperation Against Russia Aimed at Protecting Elections* (23 October 2018) // https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html
5. BBC. *US imposes new Russia sanctions over cyber-attacks*. (11 June 2018) // https://www.bbc.com/news/world-us-canada-44446449
6. Braverman, Suella. *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.* (19 May 2022) // https://www.gov.uk/government/speeches/international-law-in-future-frontiers
7. *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America).* International Court of Justice (Judgement of 27 June 1986), para. 244–245.

8. Chesney, Robert. *The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes*. (25 September 2018) // https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes
9. Council Decision 2019/797 of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States.
10. 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* // https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf
11. Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.
12. 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* // https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf
13. Dawidowicz, Martin. *Third-Party Countermeasures in International Law.* New York: Cambridge University Press, 2017, 29.
14. Department of the Prime Minister and Cabinet, New Zealand. *The Application of International Law to State Activity in Cyberspace //* https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf
15. Dohnalová, Anna, and Radek Bartoníček. *Ukrajinských hrdinů. Praha přejmenovala část ulice Korunovační u ruské ambasády.* (22 April 2022) // https://zpravy.aktualne.cz/regiony/praha/ukrajinskych-hrdinu-praha/r~92302b02c21411ec8a24ac1f6b220ee8/
16. Duguin, Stéphane, Pavlina Pavlova. *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict.* (September 2023) // https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf
17. Egan, Brian J. *International Law and Stability in Cyberspace*. (10 November 2016) // https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf
18. European Parliamentary Research Service. *Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence*. (May 2020) // https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI(2020)651937_EN.pdf
19. European Union External Action. *EU imposes first ever cyber sanctions to protect itself from cyber-attacks.* (30 July 2020) // https://www.eeas.europa.eu/eeas/eu-imposes-first-ever-cyber-sanctions-protect-itself-cyber-attacks_en
20. Federal Department of Foreign Affairs of Switzerland. *Switzerland's position paper on the application of international law in cyberspace* // https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf
21. Foreign, Commonwealth and Development Office of the United Kingdom. *Application of international law to states' conduct in cyberspace: UK statement //* 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

22. Grant, John P., and Craig J. Barker. *Parry & Grant encyclopaedic dictionary of international law.* New York: Oxford University Press, 2009, 525.
23. Giegerich, Thomas. "Retorsion". In: Rüdiger Wolfrum, ed., *Max Planc Encyclopedia of Public International Law.* Oxford: OUP, 2017.
24. Government of the Kingdom of the Netherlands. *Appendix: International law in cyberspace //* 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
25. Haataja, Samuli. *Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics.* Oxfordshire: Routledge, 2020, 180–181.
26. International Law Commission. *Yearbook of the International Law Commission: Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries.* Vol. II, part two (2001): 71–86 (hereinafter also ARSIWA).
27. Jibilian, Isabella, and Katie Canales. *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*. (15 April 2021) // https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12
28. Kosseff, Jeff. "Retorsion as a Response to Ongoing Malign Cyberoperations": 15. In: T. Jančárková, L., Lindström, M., Signoretti, I., Tolga, G., Visky, eds., *2020 12th International Conference on Cyber Conflict.* Tallinn: NATO CCDCOE Publications, 2020.
29. Lahmann, Henning. *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* Cambridge: Cambridge University Press, 2020.
30. Lotrionte, Catherine. "Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law." *The Cyber Defense Review* 3 (2018): 92.
31. McDonald, Neil, and Anna McLeod. "Antisocial Behaviour, Unfriendly Relations: Assessing the Contemporary Value of the Categories of Unfriendly Acts and Retorsion in International Law." *Journal of Conflict & Security Law* 26 (2021): 423.
32. Morello, Carol, and Ellen Nakashima. *U.S. imposes sanctions on North Korean hackers accused in Sony attack, dozens of other incidents*. (13 September 2019) // 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
33. Moret, Erica, and Patryk Pawlak. *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime? (*12 July 2017) // https://www.iss.europa.eu/content/eu-cyber-diplomacy-toolbox-towards-cyber-sanctions-regime
34. Nakashima, Ellen, and Paul Sonne. *U.S. military carried out secret cyberstrike on Iran to prevent it from interfering with shipping*. (28 August 2019) // https://www.washingtonpost.com/national-security/us-military-carried-out-secret-cyber-strike-on-iran-to-prevent-it-from-interfering-with-shipping/2019/08/28/36202a4e-c9db-11e9-a1fe-ca46e8d573c0_story.html
35. Roguski, Przemyslaw. *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views //* https://ruj.uj.edu.pl/xmlui/bitstream/

handle/item/153989/roguski_application_of_international_law_to_cyber_operations_2020.pdf?sequence=1&isAllowed=y

36. Ruys, Tom. "Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework": 24. In: Larissa van den Herik, ed., *Research Handbook on UN Sanctions and International Law.* Cheltenham: Edward Elgar Publishing, 2017.
37. Sanger, David E. *Obama Strikes Back at Russia for Election Hacking*. (29 December 2016) // https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html
38. Schmitt, Michael N. "The Law of Cyber Warfare: Quo Vadis?" *Stanford Law and Policy Review* 25 (2014): 287.
39. Schmidt, Julia. "The Legality of Unilateral Extra-territorial Sanctions under International Law." *Journal of Conflict & Security Law* 27 *(*2022): 73.
40. Schmitt, Michael N., et al. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press, 2013, 40.
41. Schmitt, Michael N. et al. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press, 2017, 82.
42. Schmitt, Michael N. "Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law." *Virginia Journal of International Law* 54 (2015): 701.
43. Schmitt, Michael N. "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: an Analytical Vade Mecum." *Harvard National Security Journal* 8 (2017).
44. Schmitt, Michael N. *Terminological Precision And International Cyber Law.* (29 July 2021) // https://lieber.westpoint.edu/terminological-precision-international-cyber-law
45. Spáčil, Jakub. "Plea of Necessity: Legal Key to Protection Against Unattributable Cyber Operations." *Masaryk University Journal of Law and Technology* 16 (2022): 218.
46. Spáčil, Jakub. "Animus Aggressionis: The Role Of Intent in the Analysis of Armed Attack in Cyberspace." *Czech Yearbook of Public & Private International Law* 13 (2022): 58–59.
47. The Federal Government of Germany. *On the Application of International Law in Cyberspace//*https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf
48. The NATO Cooperative Cyber Defence Centre of Excellence. *CCDCOE to Host the Tallinn Manual 3.0 Process.* // https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/
49. The NATO Cooperative Cyber Defence Centre of Excellence. *European Union Equipping Itself against Cyber Attacks with the Help of Cyber Diplomacy Toolbox* // https://ccdcoe.org/incyder-articles/european-union-equipping-itself-against-cyber-attacks-with-the-help-of-cyber-diplomacy-toolbox/
50. The White House. *Fact Sheet: Actions in Response to Russian Malicious Cyber Activity and Harassment*. *(*29 December 2016) // https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and

51. U. S. Department of State. *Holding Russia To Account*. (15 April 2021) // https://www.state.gov/holding-russia-to-account/
52. U.S. Department of the Treasury. *Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks.* (15 March 2018) // https://home.treasury.gov/news/press-releases/sm0312
53. U.S. Department of the Treasury. *Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups.* (13 September 2019) // https://home.treasury.gov/news/press-releases/sm0312
54. UN General Assembly Resolution 2625 from 24 October 1970. *"The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States"*.
55. 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.* // https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf
56. Valuch, Jozef, and Ondrej Hamuľák. "Use of Force in Cyberspace." *International and Comparative Law Review* 20 (2020): 174–191.
57. von Heinegg, Wolff Heintschel. "Territorial Sovereignty and Neutrality in Cyberspace." *International Law Studies* 89 (2013): 123.
58. Wallace, David, and Marc Visger. "The Use of Weaponized "Honeypots" under the Customary International Law of State Responsibility." *Cyber Defense Review* 3 (2018): 38.