DOI 10.5817/MUJLT2022-2-4

PLEA OF NECESSITY: LEGAL KEY TO PROTECTION AGAINST UNATTRIBUTABLE CYBER OPERATIONS*

by

JAKUB SPÁČIL

Cyber operations represent one of the main security threats today. The number of cyber operations attacking critical infrastructure is increasing year by year and states are looking for means to defend against this threat. However, the origin of hostile cyber operations is often located in the territory of another state, and attacked states must therefore grapple with the question of international law in their search for an effective defence mechanism. If states wish to defend themselves actively, the sovereignty of another state may be infringed, and such an infringement must be justified by an instrument of international law. These instruments of international law are retorsion, countermeasures, self-defence and plea of necessity. Application of plea of necessity, unlike the other alternatives mentioned, is not premised on the attributability of the cyber operation to the state, and it is precisely the attribution of cyber operation that poses one of the main problems of taking legal defensive measures. The article is divided into two parts. The first part is devoted to the relationship between retorsion, countermeasures, self-defence and plea of necessity. The second part discusses the conditions for the application of plea of necessity in the cyber context. The text takes into account the available state practice, in particular the national positions on the application of plea of necessity in the cyber context published in the last three years.

KEY WORDS

cyber operations, international law, plea of necessity, self-defence, cyber attack, attribution of cyber operation

* The article was written as an output of the project "Action in plea of necessity as a defence against cyber operations of non-state actors" implemented under the auspices and with the financial support of the Faculty of Law of Palacký University in Olomouc.

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.[1] In the case of a domestic cyber operation, States generally have sufficient domestic legal means to protect themselves (for example, through law enforcement 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 attacked state to defend itself against a cyber operation from a foreign state. The attacked 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.[2]

However, attribution in the technical sense is particularly problematic. While in the case of a conventional attack it is relatively easy to determine

[1] 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. (2022) *Significant cyber incidents.* [online] Washington, D. C.: CSIS. Available from: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [Accessed 3 January 2022].

the place of origin of the threat by locating the place of launch of a missile or the place of launch of bombers or inferring information about the origin from the very nature of the weapon used (e. g. missiles used by a particular State), 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.[3]

Thus, in the case of cyber operations, it is 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.[4] This is the reason why this institute has received increasing attention in recent years, not only in the scholarly debate,[5] but references to this institute are also beginning to appear in the national cyber strategies of a number of States.[6]

The aim of this paper is a detailed analysis of the plea of necessity and its applicability in the context of cyber operations. Since the plea of necessity

---

[2] International Law Commission. (2001) *Yearbook of the International Law Commission: Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*. vol. II, part two, arts. 4-11 (hereinafter "ARSIWA 2001 with commentaries"); Nicaragua v. United States of America (1986) International Court of Justice, *Case Concerning Military and Paramilitary Activities in and against Nicaragua*, paras. 105-115 (hereinafter "Nicaragua v. United States").

[3] ARSIWA 2001 with commentaries, arts. 4-11.

[4] Schmitt, M. N. (2017) Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: an Analytical Vade Mecum. *Harvard National Security Journal*, 8 (2), p. 251.

[5] 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. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press, pp. 201-257; see also Arimatsu, L. and Schmitt, M. N. (2021) The Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, pp. 1171-1198.

has not yet been invoked by any State as a circumstance precluding wrongfulness in the cyber context, the analysis builds on state practice and case law available for different contexts and suggests ways how to apply this concept in the realm of cyber operations. The paper focuses on conditions of the plea of necessity established by international law one by one and deals with the question of how should these conditions be interpreted and respected in case the plea of necessity is invoked as a justification for protective measures against a cyber operation.

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.[7] 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.[8] 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.[9]

The plea of necessity is a circumstance precluding wrongfulness (of an act of a State) and its definition can be found in Article 25 of ARSIWA. It can only be invoked as justification for an act if that act is "the only way for the State to safeguard an essential interest against a grave and imminent peril" under the condition that the act "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".[10] However, it can never be invoked in case "the international obligation in question excludes

[6] 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 [Accessed 3 January 2022].

[7] ARSIWA 2001, Art. 25 (1) (a).

[8] ARSIWA 2001 with commentaries, Art. 25, p. 80, para. 2.

[9] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97., p. 1185-1186.

[10] ARSIWA 2001, Art. 25, para 1.

the possibility of invoking necessity" or if the invoking State "has contributed to the situation of necessity".[11]

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.[12] It is an instrument which "can only be accepted on an exceptional basis"[13] and whose threshold is extremely high.[14] the exceptional nature of the plea of necessity is also confirmed by the negative wording of this article of ARSIWA.[15] The conditions of the plea of necessity stated in the definition were also confirmed by the International Court of Justice ("ICJ") in the Gabcikovo-Nagymaros judgment.[16]

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 it: "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."[17] 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, 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.[18]

A more detailed definition of the terms of the 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 the plea

---

[11] ARSIWA 2001, Art. 25, para 2.

[12] ARSIWA 2001 with commentaries, Art. 25, p. 80, para. 2.

[13] Hungary v. Slovakia (1997) International Court of Justice, Case Concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia), para. 51 (hereinafter "Gabčíkovo-Nagymaros").

[14] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, p. 135.

[15] ARSIWA 2001 with commentaries, Art. 25, p. 83, para. 14.

[16] Gabcikovo-Nagymaros, para. 51.

[17] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, p. 135.

[18] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1), p. 1624; Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, pp. 137-141.

of necessity and retorsion, countermeasures and self-defence as possible alternatives to justify protective measures against a cyber operation in order to demonstrate comparative advantages and disadvantages of the plea of necessity.

1.2 ALTERNATIVE MEASURES OF RESPONES

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".[19] 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 ban and froze the assets of six individuals and three companies in connection with the Wanna Cry, Not Petya and Cloud Hopper operations.[20]

The second option that can be used to defend against a cyber operation is 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".[21] 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 attacked 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).[22] However, invocation of countermeasures is also subject to several conditions.

---

[19] Grant, J. P. and Barker, C. J. (2009) *Parry & Grant encyclopaedic dictionary of international law*. 3rd ed. New York: Oxford University Press, p. 525 - 526.

[20] Council of the European Union. (2020) *EU Imposes the First Ever Sanctions against Cyber-Attacks.* [press release]. 30 July. Available from: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/ [Accessed 3 January 2022]; see also Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1173.

[21] ARSIWA 2001 with commentaries, Art. 22, p. 75, para. 1.

[22] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1179.

Countermeasures are only available if there is an internationally wrongful act committed by another state.[23] Thus, a prerequisite for the application of countermeasures is the attributability of the cyber operation to a state.[24] As noted above, the attributability of cyber operations is highly problematic, and countermeasures will therefore often not be available. Even if the cyber operation was attributed to a state, the countermeasures would still have to conform to other conditions: proportionality[25] and the prohibition of the threat or use of force.[26] Finally, countermeasures cannot be invoked against cyber operations launched by non-State actors, unless such conduct is attributable to the State.

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.[27] the right to self-defence is an exception to the prohibition on the use and threat of force.[28] There are three issues associated with the right to self-defence in the context of cyber operations: the possibility of self-defence against non-State actors, attribution and the threshold of an armed attack.

The issue of the invocation of self-defence against armed attacks carried out by non-State actors is highly controversial. However, genuinely analyzing this issues would be out of scope of this paper. It will therefore only be pointed out that use of force against the territory of another State on the basis of cyber operations carried out by a non-State actor whose conduct is not attributable to that State is unlikely to be accepted by the international community as a valid justification of such act.[29]

---

[23] ARSIWA 2001 with commentaries, 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."

[24] ARSIWA 2001 with commentaries, Art. 22, p. 75, para. 1.

[25] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1180.

[26] ARSIWA 2001, Art. 50(1)(a).

[27] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1), p. 1619.

[28] Charter of the United Nations, 26 June 1945, article 2 (4).

[29] For indepth analysis see Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, 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; International Court of Justice. (2004) Advisory Opinion of 9 July 2004, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, para. 139 (hereinafter "Wall Advisory Opinion").

In relation to the issue of attribution, the problem is not so much the legal attribution itself, but rather the objective demonstration of the existence of a 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.[30]

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.[31] It can be concluded that the threshold of an armed attack in the cyber context remains unclear which severely limits the possibility of invocation of self-defence against cyber operations.[32]

A repertoire of legal instruments that states may have at their disposal in the event that they fall victim to a cyber operation has been presented. Each of them has its own drawback. Alongside these legal instruments stands the plea of necessity.

The plea of necessity has several advantages over the above options. In the first place, the plea of necessity 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

---

[30] ARSIWA 2001 with commentaries, arts. 4-11.

[31] International Court of Justice. (1986) Judgment of 27 June 1986, *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, para. 191.

[32] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1175; For a detailed analysis of approaches to "armed attack" in cyberspace see VALUCH, J and HAMUĽÁK, O. (2020) Use of Force in Cyberspace. *International and Comparative Law Review*, 20 (2), pp. 174-191.

can justify measures against a non-responsible State.[33] Plea of necessity can justify even "bleed-over effects" into third States.[34] Finally, unlike countermeasures, plea of necessity is available when harm is imminent, i.e. has not manifested yet.[35] 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.[36] 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. PRECONDITIONS AND LIMITATIONS OF THE PLEA OF NECESSITY

The main objective of international law is "to maintain peace and security through a rules-based system"[37] and the creation of the United Nations was motivated primarily by the objective "to maintain international peace and security".[38] 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.[39] It is therefore logical and correct that it is an exceptional measure with a high threshold, as already mentioned above, and that the use of this institute is limited by a 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.

---

[33] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, p. 137.

[34] Ibid.

[35] Lotrionte, C. (2018) Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law. *The Cyber Defense Review*, 3 (2), p. 96.

[36] As Germany has also expressed in its official position on the application of international law in cyberspace, the plea of necessity is available "even in certain situations in which the prerequisites for countermeasures or self-defence are not met". The Federal Government Of Germany. (2021) *On the Application of International Law in Cyberspace*. [online] p. 14-15. Available from: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf [Accessed 4 January 2022].

[37] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1173.

[38] Charter of the United Nations, 26 June 1945, article 1(1).

[39] ARSIWA 2001 with commentaries, Art. 25, p. 80, para. 2; Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1), p. 1619.

2.1 PRECONDITIONS AND LIMITATIONS UNDER ART. 25 ARSIWA

2.1.1 ESSENTIAL INTEREST

A State can justify a measure on the basis of plea of necessity only if its "essential interest" is at stake.[40] 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".[41] Essential interest then undoubtedly cannot be limited to "solely a matter of the 'existence' of the State".[42] According to Tallinn Experts, it is true that "the determination of whether an interest is essential is always contextual".[43] A broader range of interests can be included among the essential interests. According to case law, these interests include protection of environment,[44] issues connected to financial obligations,[45] and protection of persons from terrorist attacks.[46] 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".[47] Schaller points out that essential interests may be interests related to "territorial integrity, political independence, and constitutional order of a State, the maintenance of public security, and the maintenance of the natural environment".[48]

If we focus on the 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

---

40 ARSIWA 2001, article 25(1)(a).

41 ARSIWA 2001 with commentaries, Art. 25, p. 83, para. 15.

42 International Law Commission. (1980) *Yearbook of the International Law Commission: Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*. vol. II, part two, p. 49, para. 32 (hereinafter "ARSIWA 1980 with commentaries").

43 Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, p. 135.

44 Gabčíkovo-Nagymaros, para. 53.

45 Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press, p. 208.

46 Lahmann derives the protection of persons from terrorist attacks as an essential interest from the advisory opinion on the Wall. See op. cit., p. 208, note 33.

47 Lotrionte, C. (2018) Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law. The *Cyber Defense Review*, 3 (2), p. 97.

48 Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1), p. 1633.

the Netherlands conceives of essential interests more broadly as "services such as the electricity grid, water supply and the banking system".[49]

It is thus clear from the case law, academic literature and state practice listed above 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 when invoking the plea of necessity.

Furthermore, the above positions of Germany and the 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.[50] 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.[51] 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 the plea of necessity cited above.[52]

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".[53] 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

---

[49] The Federal Government Of Germany. (2021) op. cit.; Government Of the Kingdom Of the Netherlands. *Appendix: International law in cyberspace*. [online] pp. 7-8. 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 [Accessed 4 January 2022].

[50] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1), p. 1632; Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, p. 135.

[51] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, pp. 135-136.

[52] Use of the phrase "certain critical infrastructure".

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.[54] 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.

2.1.2 GRAVE AND IMMINENT PERIL

Another prerequisite to acting in the plea of necessity is that the essential interest is threatened by "grave and imminent peril".[55] the ILC has stated that "[t]he peril has to be objectively established and not merely apprehended as possible".[56] This idea was elaborated by the ICJ when it stated that peril "has to be duly established at the relevant point in time".[57]

Schaller defines "peril" as "a situation in which harm is likely to occur if no preventive action is taken".[58] 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

---

[53] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1185; Conversely, Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press on p. 209 does not consider the contextual nature and considers any operation that "partially or entirely disrupts" critical infrastructure as a grave peril.

[54] Schmitt, M. N. (2017) Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: an Analytical Vade Mecum. *Harvard National Security Journal*, 8 (2), p. 252; For another example of contextual analysis of essential interest see also Arimatsu, L. And SchmittSchmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press., M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1184.

[55] ARSIWA 2001, Article 25(1)(a).

[56] ARSIWA 2001 with commentaries, Art. 25, p. 83, para. 15; Bannelier, K. and Christakis, T. (2017) *Cyber-Attacks: Preventions-Reactions: the Role of States and Private Actors*. 1st ed. Paris: Les Cahiers de la Revue Défense Nationale. p. 38.

[57] Gabčíkovo-Nagymaros, para. 54.

[58] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1), p. 1633.

or rendering it largely dysfunctional".[59] However, the risk of causing material damage or injury is not a prerequisite for grave peril.[60] 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.[61] 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 in its national strategy.[62] 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 damage 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.[63] the ILC has stated that "peril has to be imminent in the sence of proximity."[64] However, this does not mean that the imminence of the peril shall be considered only from the point of view of temporary element.[65] 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

---

[59] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University PressSchmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press., p. 136.

[60] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, p. 136; the Federal Government Of Germany. (2021) op. cit.; Government Of the Kingdom Of the Netherlands. op. cit., pp. 7-8.

[61] Ibid.

[62] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1188; The Federal Government Of Germany. (2021) op. cit.; Ministry Of Defence Of France. (2019) *International Law Applied to Operations in Cyberspace.* [online], p. 8. Available from: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf [Accessed 5 January 2022].

[63] SchmittSchmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press., M. N. (2017) Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: an Analytical Vade Mecum. *Harvard National Security Journal*, 8 (2), p. 251.

[64] ARSIWA with commentaries, Art. 25, p. 83, para. 15.

off it might be, is not thereby any less certain and inevitable".[66] 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.[67]

The Tallinn Manual 2.0 provides a number of examples of cyber operations for which the conditions of the 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".[68]

2.1.3 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".[69] Such alternatives may be purely technical solutions (e.g.

[65] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University PressSchmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press., p. 138.

[66] Gabcikovo-Nagymaros, para. 54.

[67] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, p. 139; see also Arimatsu, L. And SchmittSchmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press., M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1190 and Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1), p. 1636.

[68] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, p. 136.

[69] ARSIWA 2001 with commentaries, Art. 25(1)(a), p. 83, para. 15; see also Arimatsu, L. And SchmittSchmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press., M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1192;

moving operations from the damaged infrastructure to other available infrastructure),[70] the use of diplomatic procedures (see retorsion above), solutions through international organizations (e.g. referring the matter to the UN Security Council)[71] or other procedures, such as those listed in the Cyber Toolbox of the European Union.[72]

It is the "only mean available" condition that most often prevents the invocation of the plea of necessity.[73] 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.[74] the ICJ reached the same conclusion in Wall Advisory Opinion.[75] 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 (e. g. defensive cyber measures on the territory of the USA such as "sinkholing" the command and control domain of the malware).[76]

The importance of this condition is also evidenced by the fact that four of the six national positions mentioning the plea of necessity explicitly or

---

[70] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, p. 139.

[71] ARSIWA 2001 with commentaries, Art. 25, p. 83, para. 15; Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, p. 141.

[72] Council Of the European Union. (2017) *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")* [online]. 10474/17, pp. 3-5. Available from: https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf [Accessed 5 January 2022]; see also Schweighofer, E., Brunner, I. and Zanol, J. (2020) 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*, 14 (2), p. 252.

[73] Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press, p. 216.

[74] Gabčíkovo-Nagymaros, para. 55.

[75] Wall Advisory Opinion, para. 140.

[76] Schmitt, M. (2020) *Top Expert Backgrounder: Russia's SolarWinds Operation and International Law.* [online] New York: Just Security. Available from: https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/ [Accessed 5 January 2022].

implicitly (by reference to the terms of Article 25 of ARSIWA) mention this condition. These are Japan,[77] the Netherlands,[78] Norway[79] and Switzerland.[80]

2.1.4 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".[81] A prerequisite for the 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.[82] This idea is well captured by Schmitt when he stated that "states are precluded from addressing necessity situations if doing so would place any other state in comparable peril".[83] 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.[84] However, a different interpretation of Article

---

[77] Ministry Of Foreign Affairs Of Japan. (2021) *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations.* [online], p. 5. Available from: https://www.mofa.go.jp/files/100200935.pdf [Accessed 5 January 2022].

[78] Government Of the Kingdom Of the Netherlands. op. cit., p. 7-8.

[79] United Nations. (2021) *Official compendium of voluntary national contributions.* [online]. Doc. A/76/136, 13 July 2021, p. 73. Available from: https://ccdcoe.org/uploads/2018/10/UN_-Official-compendium-of-national-contributions-on-how-international-law-applies-to-use-of-ICT-by-States_A-76-136-EN.pdf [Accessed 7 January 2022].

[80] Federal Department Of Foreign Affairs Of Switzerland. (2021) *Switzerland's position paper on the application of international law in cyberspace.* [online], p. 7. Available from: https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf [Accessed 5 January 2022].

[81] ARSIWA 2021 with commentaries, Art. 15(1)(b).

[82] 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.

[83] Schmitt, M. N. (2017) Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: an Analytical Vade Mecum. *Harvard National Security Journal*, 8 (2)., p. 253;

[84] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Arimatsu, L. And SchmittSchmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press., M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1193.

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.[85]

2.1.5 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. [86]

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 these treaties containing their own plea of necessity regime which applies as lex specialis to the customary plea of necessity.[87] 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".[88] 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 preclude the applicability of the plea of necessity.[89] 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

---

[85] Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press, p. 221.

[86] ARSIWA 2001 with commentaries, Art. 25(2).

[87] ARSIWA 2001 with commentaries, Art. 25, p. 84, para. 19; Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press, p. 225.

[88] ARSIWA 2021 wtih commentaries, Art. 25, p. 84, para. 20.

[89] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, p. 140.

in connection with inadequate security of cyberinfrastructure, the State does not have the ability to apply the plea of necessity, seems questionable.[90] 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 highest level of cyber security does not guarantee perfect protection. Secondly, the scale of cyber infrastructure in use in the public and private sectors and the limited capacity of a 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 the plea of necessity as a justification for measures taken in the context of cyber operations and it should therefore be refused.

2.2 LIMITATION OF PLEA OF NECESSITY NOT MENTIONED IN ART. 25 OF ARSIWA

States are limited in their right to invoke the 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 the plea of necessity and the prohibition on use of the plea of necessity as a justification for a violation of a peremptory norm of international law under article 26 of ARSIWA.

First, let us 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".[91] 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. "[92] Some authors have subsumed the proportionality aspect under the condition of "only means available", but such a subsumption is not

[90] Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press, p. 228.

[91] ARSIWA 1980 with commentaries, Art. 33, pp. 49-50, para. 33.

[92] Ibid.

appropriate.[93] While the "only means" condition requires the selection of the most appropriate of the alternative measures, 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. [94]

Another condition limiting the repertoire of remedies available on the basis of the plea of necessity is found in Article 26 of ARSIWA, according to which "circustances precluding wrongfulness" including the plea of necessity cannot justify a violation of a peremptory norm of international law.[95] 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.[96] Which other rules of international law are peremptory norms is left to further interpretation by the ILC.[97] 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.[98] 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

---

[93] See Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press.Response Option to Hostile Cyber Operations. *International Law Studies*, 97 Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1192; Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press, p. 218.

[94] Grant, J. P. and Barker, C. J. (2009) *Parry & Grant encyclopaedic dictionary of international law*. 3rd ed. New York: Oxford University Press., pp. 549 - 550.

[95] ARSIWA 2001, Art. 26.

[96] ARSIWA 1980, Art. 33, p. 50, para. 37.

[97] Ibid.

of international law is to maintain international 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 the 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 state. 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.

3. 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. The 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.[99]

The core of this paper dealt with conditions of invocation of the plea of necessity. It was demonstrated that the first two conditions, i. e. (1) peril to the essential interest of a State which is (2) grave and imminent, do not pose a major challenge. Regarding these two conditions, it should only be pointed out that evaluation of the cyber operation has to be context dependent taking into account not just the nature of the target (e. g. hospital

[98] See e.g. Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, p. 140; Vidmar, J. (2017) the Use of Force as a Plea of Necessity. *American Journal of International Law Unbound*, 111, pp. 301-306; Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, pp. 1193-1194; Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press, pp.; Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1), p. 1621; Bannelier, K. and Christakis, T. (2017) *Cyber-Attacks: Preventions-Reactions: the Role of States and Private Actors*. 1st ed. Paris: Les Cahiers de la Revue Défense Nationale, p. 97.

[99] Lotrionte, C. (2018) Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law. The *Cyber Defense Review*, 3 (2), p. 96; Ohlin, J., D. and May, L. (2016) *Necessity in International Law*. 1st ed. New York: Oxford University Press. p. 39.

information system) but also the potential or actual consequences (a minor inconvenience compared to the death of patients).

On the contrary, the fact that the plea of necessity is only available if there are no other means applicable will prevent the invocation of this legal institute in most of scenarios. Generally, in the case of an unfriendly cyber operation victim States have at their disposal several protective measures (technical, diplomatic, and other) which do not require a breach of international law necessitating justification (in the form of the plea of necessity). If any of these measures can be used without invocation of the plea of necessity to effectively protect the essential interest against grave and imminent peril, they shall be used.

Another condition limiting the plea of necessity is the requirement not to breach the essential interest of another State including the State from whose territory the threat emanates. Two approaches were demonstrated. The first approach prohibits any interference with the essential interest of another State while the second approach uses proportionality as a criterion to distinguish between legal and illegal measures. The author of this paper is inclined to support the second approach which seems to more appropriately (fairly, if you wish) reflect the mutual rights and obligations among concerned States.

A victim State is also precluded from invoking the plea of necessity if it contributed to the peril by its own action or omission. In the paper, it was argued for the position that mere lack of up-to-date cyber security protection on the attacked computer system does not per se rule out the plea of necessity as such strict interpretation of the "contribution" condition would lead to the practical inapplicability of the necessity in the cyber context.

Probably the most important argument developed in this paper deals with the question of whether the plea of necessity can be used to justify the use of force. Even though authors arguing for legality of such approach can be found, in the present paper it was strongly argued for the opposite. Use of force is prohibited by a peremptory norm of international law. It was demonstrated with reference to the work of the ILC that the plea of necessity was never meant to justify a breach of peremptory norms and the prohibition of the use of force in particular. Only this conclusion is in line with the main objectives of the United Nations – to maintain

international peace and security. A different conclusion would unjustifiably raise the risk of escalation of the conflict.

Finally, in the analysis of the plea of necessity and prerequisites of its applicability in cyberspace attention was also paid to the state practice. So far, six states have officially announced their positions on the applicability of the plea of necessity in cyberspace and all of them agreed that, under strict conditions, the plea of necessity will be available. It can be expected that more states with a similar position will be forthcoming.

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. To avoid such risk it is necessary to respect the condition of the plea of necessity summarized above and to continue the discussion on the interpretation of these conditions in the realm of cyber operations because the plea of necessity is here to stay.

LIST OF REFERENCES

[1] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97.

[2] Bannelier, K. and Christakis, T. (2017) *Cyber-Attacks: Preventions-Reactions: the Role of States and Private Actors*. 1st ed. Paris: Les Cahiers de la Revue Défense Nationale.

[3] Center for Strategic & International Studies. (2022) *Significant cyber incidents.* [online] Washington, D. C.: CSIS. Available from: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [Accessed 3 January 2022].

[4] Council Of the European Union. (2017) *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")* [online]. 10474/17, pp. 3-5. Available from: https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf [Accessed 5 January 2022].

[5] Council of the European Union. (2020) *EU Imposes the First Ever Sanctions against Cyber-Attacks.* [press release]. 30 July. Available from:

https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/ [Accessed 3 January 2022].

[6] Federal Department Of Foreign Affairs Of Switzerland. (2021) *Switzerland's position paper on the application of international law in cyberspace.* [online], p. 7. Available from: https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf [Accessed 5 January 2022].

[7] Government Of the Kingdom Of the Netherlands. *Appendix: International law in cyberspace.* [online] pp. 7-8. 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 [Accessed 4 January 2022].

[8] Grant, J. P. and Barker, C. J. (2009) *Parry & Grant encyclopaedic dictionary of international law*. 3rd ed. New York: Oxford University Press.

[9] *Charter of the United Nations,* 26 June 1945.

[10] International Court of Justice. (1986) Judgment of 27 June 1986, *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*.

[11] International Court of Justice. (1997) Judgement of 25 September 1997, *Case Concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia).*

[12] International Court of Justice. (2004) Advisory Opinion of 9 July 2004, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory.*

[13] International Law Commission. (1980) *Yearbook of the International Law Commission: Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*. vol. II, part two.

[14] International Law Commission. (2001) *Yearbook of the International Law Commission: Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*. vol. II, part two.

[15] Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press.

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

[17] Ministry Of Defence Of France. (2019) *International Law Applied to Operations in Cyberspace.* [online], p. 8. Available from: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf [Accessed 5 January 2022].

[18] Ministry Of Foreign Affairs Of Japan. (2021) *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations.* [online], p. 5. Available from: https://www.mofa.go.jp/files/100200935.pdf [Accessed 5 January 2022].

[19] Ohlin, J., D. and May, L. (2016) *Necessity in International Law*. 1st ed. New York: Oxford University Press.

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

[21] Schmitt, M. (2020) *Top Expert Backgrounder: Russia's SolarWinds Operation and International Law.* [online] New York: Just Security. Available from: https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/ [Accessed 5 January 2022].

[22] Schmitt, M. N. (2017) Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: an Analytical Vade Mecum. *Harvard National Security Journal*, 8 (2).

[23] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press.

[24] Schweighofer, E., Brunner, I. and Zanol, J. (2020) 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*, 14 (2).

[25] The Federal Government Of Germany. (2021) *On the Application of International Law in Cyberspace.* [online] p. 14-15. Available from: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf [Accessed 4 January 2022].

[26] United Nations Security Council, Resolution 1368 (2001) adopted on 12 September 2001.

[27] United Nations Security Council, Resolution 1373 (2001) adopted on 28 September 2001.

[28] United Nations. (2021) *Official compendium of voluntary national contributions*. [online]. Doc. A/76/136, 13 July 2021, p. 73. Available from: https://ccdcoe.org/uploads/2018/10/UN_-Official-compendium-of-national-contributions-on-how-international-law-applies-to-use-of-ICT-by-States_A-76-136-EN.pdf [Accessed 7 January 2022].

[29] United Nations. (2021) *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. Available from: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf [Accessed 7 January 2022].

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

[31] Vidmar, J. (2017) the Use of Force as a Plea of Necessity. *American Journal of International Law Unbound*, 111.