KRAKOWSKIE STUDIA MIĘDZYNARODOWE
KRAKOW INTERNATIONAL STUDIES
XIX: 2022 nr 1 e-ISSN 2451-0610 ISSN 1733-2680

https://doi.org/10.48269/2451-0610-ksm-2022-1-004

Ewa Suwara
Ministry of Foreign Affairs Republic of Poland
https://orcid.org/0000-0001-7724-2620

Cyber operations and Article 42.7 of the Treaty on European Union

Introduction

Over the last few decades, operations in cyberspace and their relevance to *jus ad bellum* have become a subject of interest for scholars and practitioners coming from civilian and military backgrounds. Several major cyber operations have contributed to raising the level of interest in those activities[1]. The threat posed by the occurrence of cyber-attacks continues to be a challenge to national security. Such attacks may target and disturb the functioning of information systems, computer networks and air defense systems, as well as critical infrastructure like nuclear and electric power plants. The specificity of malicious cyber-operations comes from the immense harm they can cause to a victim state without producing any physical injuries or damage. The absence of physical effect raises the question of the qualification of cyber operations

[1] For an indicative list, see: *Significant cyber incidents since 2006*, Center for Strategic and International Studies, https://csis-website-prod.s3.amazonaws.com/s3fs-public/220805_Significant_Cyber_Events_0.pdf?ruYyPiNzwADjystZd.g9QgMEPY1K28Et [accessed: 29.08.2022].

having severe consequences as armed attacks or, (in the case of EU law) as armed aggression. As rightly outlined by the European Commission, "the emerging cyber-threat landscape is a global threat as no one is immune to cyber and hybrid attacks, and it challenges the basic principles on which our multilateral order has been built"[2].

Since the number of malicious cyber-operations has increased in recent years, there have been more arguments voiced for the recognition of a cyber-attack in international law as an exemption to the prohibition of the use of force on the grounds of Article 51 of the UN Charter. Some have even suggested that cyber-attacks should be treated as acts of war, although others argue that 'the law of war provides a useful framework for only the very small number of cyber-attacks that amount to an armed attack or that take place in the context of an ongoing armed conflict'[3].

Not every cyber-operation constitutes a cyber-attack. Not every cyber-attack is an act of armed aggression or of armed attack[4]. Not every act of armed aggression is an armed attack[5]. Finally, an armed attack and an armed aggression are not threats *per se*. A threat means 'an expression of intention to inflict evil, injury, or damage'[6]. Both terms, 'attack' and 'aggression', are characterised by a hostile action, and not just intention. However, it is internationally agreed that the threat to use force can be considered an 'attack' in the meaning of the UN Charter[7] under certain conditions[8]. Moreover, "all armed

---

2 M. Schinas, *Keynote speech of the European Commission Vice President*, 17.02.2022, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_1163 [accessed: 20.02.2022].

3 O.A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, J. Spiegel, *The Law of Cyber-Attack*, "California Law Review" 2012, Vol. 100, No. 4, p. 817.

4 M.N. Schmitt, *The use of cyber force and international law*, [in:] *The Oxford Handbook of the Use of Force in International Law*, ed. M. Weller, Oxford University Press, Oxford 2017, p. 1119.

5 Y. Dinstein, *Aggression*, [in:] *Max Planck Encyclopedia of Public International Law*, 09.2015, https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e236 [accessed: 19.02.2022].

6 *Threat* [term], [in:] *Merriam-Webster Dictionary*, www.merriam-webster.com/dictionary [accessed: 11.02.2022].

7 Article 2(4) of the UN Charter states that 'All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations', see: Article 2(4), https://legal.un.org/repertory/art2/english/rep_supp7_vol1_art2_4.pdf [accessed: 13.01.2022].

8 For more details on what constitutes a threat of force see: F. Dubuisson, A. Lagerwall, *The threat of the use of force and ultimate*, [in:] *The Oxford Handbook*..., *op. cit*.

attacks are uses of forces, but not all uses of forces are armed attacks"[9]. 'Threat', 'attack', 'aggression', 'weapon', a notion of 'aggressor' and of a 'victim' – those terms should be examined closely when assessing the relevance of existing legal instruments to some of the incidents taking place nowadays.

While there is a vast literature on cyber-attacks under traditional *jus ad bellum*[10] that grants victims of such actions the right of self-defence governed by the provisions of the UN Charter, there has been a little academic attention given to such malicious cyber-operations in the context of the European security architecture.

Faced with complex and diverse crises, the European Union (EU) has improved its response capacities over last decades through several arrangements that include establishing an Integrated Political Crisis Response[11], Emergency Response Coordination Center[12], as well as the adoption of some legal provisions such as solidarity clause in Article 222 of the Treaty on the Functioning of the European Union (TFEU)[13], allowing to enhance cooperation between the member states and the EU institutions in case of a crisis[14]. On December 16, 2020, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented new EU Cybersecurity Strategy aiming to strengthen a collective resilience against cyber threats[15]. The document recommended a reflection on the interaction between the cyber diplomacy toolbox[16]

[9] M.N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, [in:] *4th International Conference on Cyber Conflict*, eds C. Czosseck, R. Ottis, K. Ziolkowski, NATO CCDCOE Publication, Tallin 2012, p. 286, and *idem*, *The use of cyber force*..., *op. cit.*, p. 1119.

[10] Law applicable when a state resorts to force.

[11] *How does the Integrated Political Crisis Response (IPCR) mechanism work?*, Council of the EU, 2018, www.consilium.europa.eu/media/45843/ipcr-mechanism.pdf [accessed: 10.01.2022].

[12] *European Civil Protection and Humanitarian Aid Operations*, European Commission, https://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en [accessed: 10.01.2022].

[13] Consolidated Version of the Treaty on European Union [2007], OJ. C. 326., 26.10.2012, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT [accessed: 15.12.2021].

[14] P. Pawlak, *Cybersecurity and Cyberdefence EU Solidarity and Mutual Defence Clauses*, 06.2015 www.europarl.europa.eu/RegData/etudes/BRIE/2015/559488/EPRS_BRI(2015)559488_EN.pdf [accessed: 15.12.2021].

[15] *Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade*, High Representative of the Union for Foreign Affairs and Security Policy, 16.12.2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&rid=8 [accessed: 1.06.2022].

[16] Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), Document 9916/17,

and the possible use of Article 42.7 TEU[17]. The strategy was complemented by the European Commission's proposal of two directives: a revised Directive on measures for a high common level of cybersecurity across the Union repealing Directive (EU) 2016/1148[18], and a new Directive on the resilience of critical entities[19]. As indicated by the Commission, they would cover a wide range of sectors and aim to address current and future online and offline risks, from cyberattacks to crime or natural disasters[20].

In 2019, for the first time in the history, the EU introduced a legal framework allowing to impose restrictive measures on individuals and entities responsible for, or involved in, cyber-attacks affecting the EU and its Member States[21]. All this complements the existing EU legal framework.

A clause known as a 'mutual defence clause'[22], a 'mutual assistance clause'[23], or 'aid and assistance clause'[24], introduced into Article 42(7) of the

General Secretariat of the Council, 7.06.2017, https://ccdcoe.org/uploads/2018/11/EU-170607-CyberDiplomacyToolbox-1.pdf [accessed: 13.06.2022].

17 *Joint Communication to the European Parliament*..., *op. cit*.

18 Draft Directive of the European Parliament, and the Council on measures for high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, European Commission, 16.12.2020, https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union [accessed: 1.02.2022].

19 Draft Directive of the European Parliament and of the Council on the resilience of critical entities, COM/2020/829, European Commission, 16.12.2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN [accessed: 1.02.2022].

20 *New EU Cybersecurity Strategy, and new rules to make physical and digital critical entities more resilient*, European Commission, 16.12.2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391 [accessed: 1.02.2022].

21 Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, Official Journal L 129I, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2019:129I:FULL&from=EN [accessed: 20.02.2022]; Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, Official Journal L 129I, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2019:129I:FULL&from=EN [accessed: 20.02.2022].

22 *Mutual defence clause (Article 42.7 TEU)*, European Parliament, www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede200612mutualdefsolidarityclauses_/sede200612mutualdefsolidarityclauses_en.pdf [accessed: 15.12.2021].

23 J. Rehrl, *Invoking the EU's Mutual Assistance Clause. What it says, what it means*, Egmont Institute, 20.11.2015, www.egmontinstitute.be/invoking-the-eus-mutual-assistance-clause-what-it-says-what-it-means [accessed: 14.01.2022].

24 A term preferred by the author and used within this publication as it reflects the content of the provision stipulated in Article 42(7) of the Treaty on European Union.

Treaty of EU (TEU)[25] has also been a part of this long process. It is not an 'equivalent' to Article 5 of the North Atlantic Treaty[26], although it is interpreted as such[27].

Article 42(7) TEU states that "if a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States. Commitments and cooperation in this area shall be consistent with commitments under the North Atlantic Treaty Organisation, which, for those States which are members of it, remains the foundation of their collective defence and the forum for its implementation"[28].

The main objective of this publication is to examine potential conditions for the application of Article 42(7) TEU in case of cyber-operations. This objective translates into searching for answers to the questions that are fundamental to this research:

- Can Article 42(7) TEU apply to cyber operations?
- When does a cyber operation rise to the level of 'armed aggression' in the meaning of Article 42(7) TEU?

To achieve the objective, the author first takes a closer look at the content of Article 42(7) TEU, clarifying the legal obligation introduced into this provision. The notion of 'victim', 'weapon', 'territory' and 'attacker' (as well as an 'aggressor') in the context of cyber operations is analyzed, using international and EU laws as points of reference. Such a 'dismantling' of Article 42(7) TEU allows

[25] Consolidated Version of the Treaty on European Union..., *op. cit*.

[26] Article 5 of the North Atlantic Treaty states: 'The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the UN Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security'. See: North Atlantic Treaty, Washington D.C. 4.04.1949, www.nato.int/cps/en/natolive/official_texts_17120.htm [accessed: 13.12.2021].

[27] P. Pawlak, *Cybersecurity and Cyberdefence EU Solidarity*..., *op. cit.*, p. 6.

[28] Consolidated Version of the Treaty on European Union..., *op. cit*.

for its better understanding in the cyber context. 'Armed attack' and 'armed aggression' are used as points of reference for a discussion on cyber operations in the context of Article 51 of the UN Charter and Article 42(7) TEU.

Despite the European Parliament's appeals for detailed and practical analysis of Article 42(7) TEU[29], so far, academic response and reactions from the EU member states have been relatively limited. While focusing on one of the aspects of this Treaty provision, namely the application of the clause to cyber-attacks, this publication is a part of broader, ongoing post-doctoral research on Article 42(7) TEU. In this sense, the publication constitutes a preliminary contribution to further academic research on the subject.

The content of Article 42(7) of the Treaty on European Union

Article 42(7) TEU is placed in section 2 of title V TEU referring to the Common Foreign and Security Policy. In the first part, the provision introduces a legally binding obligation to provide aid and assistance that is imposed on the EU member states. Such a conclusion derives from the words 'the other Member States shall have [...] an obligation of aid and assistance'. Since it refers to aid and assistance but without indicating their form, character and method of delivery, Article 42(7) of the Treaty on European Union is not a classical mutual defence clause[30]. It does not oblige other EU member states to defend the victim state. The clause expresses the commitment of the EU member states to assist each other in the face of common danger, and it signals that certain hostile actions will be met with a unified response[31]. It therefore acts as a promise and a warn-

[29] Resolution on the mutual defence clause (Article 42(7) TEU), 2015/3034(RSP), European Parliament, 21.01.2016, point 6 and 7, www.europarl.europa.eu/doceo/document/TA-8-2016-0019_EN.pdf [accessed: 15.12.2021].

[30] Cf Article 5 of the Washington Treaty: "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the UN Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security." See: North Atlantic Treaty..., *op. cit*.

[31] A. Sari, *The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats*, "Harvard National Security Journal" 2019, Vol. 19, p. 410.

ing[32]. However, it remains unclear whether the assisting member states may only act within the scope of the request and whether the request should specify the quantity and type of aid. The clause does not indicate a procedure to ask for such assistance, and such a request is not considered as a condition for receiving aid and assistance from other EU member states.

It is clear that the decision on the form, character, and method of delivery of aid and assistance is up to member states and shall be read jointly with Article 3 of the Irish Protocol providing that it "will be for Member States – including Ireland, acting in a spirit of solidarity and without prejudice to its traditional policy of military neutrality – to determine the nature of aid or assistance to be provided to a Member State which is the object of a terrorist attack or the victim of armed aggression on its territory"[33]. This formulation confirms that the clause is of an intergovernmental character, and it does not require the transfer of competences or engagement of the EU institutions.

However, based on Article 42(4) TEU, the High Representative may be involved in launching the application of the aid and assistance clause. Like the EU victim member state, it could submit a request to the Council to classify a given act as an 'armed aggression' in the sense of Article 42(7) TEU[34]. The clause does not determine who decides whether a member state has become a victim of armed aggression on its territory. As Article 42(7) TEU does not fall under the jurisdiction of the European Court of Justice, it may be assumed that interpretation of its content falls under the responsibility of each member state. It is both political and normative in nature. Lack of consensus on interpretation among the member states of the EU does not affect the right of each of the member states to identify itself as a victim. Yet, Article 31(4) TEU stipulates that any decisions with military or defence implications require unanimity of the Council. In practical terms, it means, that in the event of an invocation of Article 42(7) TEU and a request for military or defence means and tools, every EU member state has a right to assess the occurrence of armed aggression. There is no clear guidance on the procedure of assessment when no military and defense tools are involved.

---

[32] *Ibidem*.

[33] Protocol on the concerns of the Irish people on the Treaty of Lisbon, Official Journal of the European Union L 60/131, 2.03.2003, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2013_060_R_0129_01&rid=3 [accessed: 13.01.2022].

[34] E. Suwara, *Klauzula wzajemnej pomocy i wsparcia zawarta w art. 42 ust. 7 Traktatu o Unii Europejskiej*, "Państwo i Prawo" 2018, nr 7, p. 91.

It is also worth noting that the first part of the clause explains the relationship to Article 51 within Chapter VII of the UN Charter. The obligation of aid and assistance provided by the EU member states to the victims of armed aggression comes from the inherent right of (individual or collective) self-defence.

It remains unquestionable that the fundamental objective of the UN Charter is to maintain international peace and security, while the main purpose of Article 51 of the UN Charter is to provide effective protection to the attacked state through the exercise of the right of self-defence against the aggressor. It seems that by a direct reference to the content of the UN Charter, the EU and its Treaty refer to the UN Charter as a framework for any acts of armed aggression occurring on the territory of the EU member states. In such a context, with the UN Charter aiming to maintain international peace and security, the three main objectives of Article 42(7) TEU include cooperation among the EU member states and the provision of aid and assistance to the EU victim state(s), as well as strengthening of the unity of the EU. The explanation of such relationship is of importance, especially when contemplating the application of Article 42(7) TEU to cyber operations that have been subjected to analysis against Article 51 of the UN Charter.

There is a general rule in international law that prohibits the use of force in international relations as reflected in Article 2(4) of the UN Charter. There are two exceptions to it, one provided in Article 39 of the UN Charter, when the measures involving the use of force are authorized by the UN Security Council, and the other one, foreseen in Article 51 of the UN Charter, permitting the affected state to exercise, under certain conditions, the right of self-defence. Article 42(7) TEU directly refers to Article 51 of the UN Charter.

While the EU member state exercises the right of self-defence provided in Article 51 of the UN, in case of armed aggression on the EU territory, and based on Article 42(7) TEU, the other EU member states have obligation to aid and assist it in all the means in their power. In other words, it is UN Charter that gives – under certain conditions – the right of exercising the self-defence and permission to use of force against armed attack to the affected state, and not Article 42(7) TEU. The role of Article 42(7) TEU is, in that sense, complementary to the UN Charter. Article 42(7) TEU focuses only on the obligation to provide aid and assistance.

If one accepts such an approach at first, there is a need to establish whether the incident rises to the level of 'an armed attack' in the meaning of Article 51 of the UN Charter. If the affected state may legitimately exercise the right of self-defence based on Article 51 of the UN Charter, the other EU member states have the obligation to aid and assist with all the means in their power.

As the content of Article 42(7) TEU includes the notion of 'armed aggression' in some of the EU language versions, there is a need to confront the incident with this term. In the cyber context, it means that cyber operations require the assessment against the conditions of Article 51 of the UN Charter, followed by the assessment against the conditions foreseen by Article 42(7) TEU.

Notion of a 'victim' in context of 'cyber operations'

Although Article 51 of the UN Charter does not include the term 'victim', some official language versions of Article 42(7) TEU make a direct reference to it. Approximately seven language versions of Article 42(7) TEU[35] mention 'victim', ten use the formula 'subject to / object to / subjected to'[36], while the remaining seven do not point to any of them[37].

There is no commonly agreed definition of a victim in the international law[38]. A victim means 'one that is acted on and usually adversely affected by a force or agent'[39]. It may appear that a victim may be a physical person or legal entity – individually or collectively, state institution(s), as well as privately owned entities, if the state concerned claims to be adversely affected by such attack. However, to be a victim of an armed attack or aggression in the meaning of international law requires the fulfilment of additional conditions relative to the notion of an armed attack as such.

Being a victim, as stipulated in Article 42(7) TEU, leads to the assumption that the act(s) of the aggression has occurred, or it is ongoing[40], adversely

35 EE, EN, HR, LV, MT, PL, SK.

36 BG, ES, CZ, DK, FI, FR, IT, NL, RO, SE.

37 DE, EL, GA, HU, LT, PT, SI.

38 The notion of 'victim' is considered by several international legal instruments and rests undefined. As pointed out by CF de Casadevante Romani 'ways of considering the Victims differ in human rights law, in international criminal law and international humanitarian law'. For more on the notion of 'victim', see: C.F. de Casadevante Romani, *International Law of Victims*, "Max Planck Yearbook of United Nations Law" 2010, Vol. 14, pp. 219–272.

39 *Victim* [term], [in:] *Merriam-Webster Dictionary*, *op. cit*.

40 In the French version of the text, it is written 'au cas où un État membre serait l'objet d'une agression armée sur son territoire'– which translates into the following words: "in the event that a member State is the object of armed aggression on its territory". While there is no discrepancy in framing the time of aggression between the French and English version, the word 'victim' is replaced by 'an object of'. 'An object' is something mental or physical toward which thought, feeling, or action is directed. See: *An object* [term], [in:] *Merriam-Webster Dictionary*, *op. cit*.

affecting EU member state. Such an assumption may have an impact on defining the moment of the attack and thus on the time at which the right to self-defence arises (and especially in relation to the potential threat of using force). There is no consensus on the subject[41]. Further analysis may require confronting the issue of 'imminence' with the notion of 'victim', especially in cases when concepts of anticipatory and pre-emptive self-defence are considered. The International Court of Justice indicated in the case of the Islamic Republic of Iran vs. the United States of America that the obligation to prove the existence of an attack rests on the country which exercised the right of self-defence[42]. In the case of Nicaragua v. the United States of America, the Court underlined that the evidence needs to be adequate and direct[43].

The concept of pre-emptive self-defence and the concept of anticipatory self-defence continue to be the subject of discussion among scholars[44] and it is relevant for the discussion within the scope of this research. Under customary law, anticipatory self-defence is permissible when the threat of an armed attack is 'imminent'[45]. It refers to a concrete, impending future attack. On the other hand, pre-emptive self-defence refers to attacks that are non-imminent, and it is much broader than anticipatory self-defence, as it aims at halting a potential and abstract future armed attack, where there is no actual plan of attacking. In other words, if the moment of a future attack is so close that it is no longer avoidable, then self-defence from preventive becomes pre-emptive[46]. In this context, as stipulated in Article 42(7) TEU being a 'victim of armed aggression' (the aggression is occurring, or it has occurred) in its

41 A. Randelzhofer, [in:] *The UN Charter of the United Nations, a commentary*, eds B. Simma, D.-E. Khan, G. Nolte, A. Paulus, N. Wessendorf, 3th ed., Vol. 1, Oxford University Press, Oxford–New York 2012, p. 1421.

42 Case concerning oil platforms Islamic Republic of Iran v. United States of America, ICJ Reports 2003, para 64 and 72, International Court of Justice, www.icj-cij.org/en/case/90 [accessed: 30.11.2021].

43 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), International Court of Justice, ICJ Reports 1986, para 11 and 109, www.icj-cij.org/en/case/70/judgments [accessed: 30.11.2021].

44 There is also concept of preventive self-defence. A.S. Deeks, *Taming the doctrine of pre-emption*, [in:] *The Oxford Handbook*..., *op. cit*.

45 N.A. Shah, *Self-defence Anticipatory Self-defence, and Pre-emption: International Law's Response to Terrorism*, "Journal of Conflict and Security Law" 2017, Vol. 12, Issue 1, p. 100.

46 V. Upeniece, *Conditions for the legal commencement of an armed attack*, [in:] *6th International Interdisciplinary Scientific Conference Society. Health. Welfare. 23–25 November 2016, Riga*, ed. U. Berkis *et al.*, EDP Sciences, 2018, p. 5.

literal meaning[47] may exclude the relevance and application of anticipatory and pre-emptive self-defence, when the status of an affected state does not necessarily qualify into such category[48]. It could be agreed, that if an armed attack or aggression has not occurred, then the state cannot yet be considered a 'victim' of it.

However, if such an approach is accepted within the meaning of Article 42(7) TEU, it would then partially contradict the trend in the interpretation of Article 51 of the UN Charter when it comes to pre-emptive and anticipatory self-defence. Moreover, it would likely oppose Article 2(4) of the UN Charter, which explicitly indicates a threat to use armed force as a ground to refer to the right of self-defence. Literally, the threat to use armed force may not necessarily be sufficient to identify a state as a victim of armed attack or armed aggression, since the threat does provide for being affected by force.

Surely, the issue of the notion of victim in the meaning of Article 42(7) TEU requires further consideration, as it is of significance also for cyber operations. "Given the speed and complexity of cyber-attacks, requiring a state to wait until there is 'no moment for deliberation' before responding with force increasingly looks like a requirement that a state should stand by and suffer an attack"[49]. This puts additional pressure on the concept because of the nature of the (cyber) threat, potential gravity of the harm, as well as a speed with which the attack would arrive once launched[50], impacting the status of a state as a 'victim' state.

Moreover, in the case of cyber-attacks, it may happen that the victim state may not be aware that it is under attack. In such a case, "its right to respond in self-defence will only persist if the attacks are likely to continue"[51].

Notion of a 'weapon' in the context of cyber operations

There is no generally accepted legal definition of a 'weapon' under international law[52], that may be applied to 'armed aggression' as provided in Article

[47] In such a definition a victim refers to 'one that is injured, destroyed, or sacrificed under any of various conditions'; *victim* [term], [in:] *Merriam-Webster Dictionary*, *op. cit.*

[48] Some (i.e., Ian Brownlie and Philip Jessup) underline that the right of self-defence does not exist if an armed attack has not yet occurred. See: I. Brownlie, *International law, and the Use of Force by States*, Clarendon Press, Oxford 1963, p. 278; P. Jessup, *A Modern law of Nations*, Archon Books, Hamden CT 1968, p. 166.

[49] A.S. Deeks, *Taming the doctrine*..., *op. cit.*, p. 670.

[50] *Ibidem*.

[51] M.N. Schmitt, *The use of cyber force*..., *op. cit.*, p. 1127.

[52] G.H. Todd, *Armed attack in cyberspace: deterring asymmetric warfare with an asymmetric definition*, "The Air Force Law Review" 2009, Vol. 19, p. 80.

42(7) TEU. The notion of 'armed' understood literally as 'using or carrying weapons'[53] requires closer look into the definition of 'weapon', and its relevance for attribution of acts as armed aggression. The International Committee of the Red Cross (ICRC) pointed out that 'each state tends to have its own definition of 'weapon'[54]. A weapon may be defined as 'a thing designed, intended, or used for inflicting bodily harm or physical damage; a means of gaining an advantage or defending oneself'[55].

According to the Tallin Manual, 'cyber weapons' are "cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, which result in the consequences required for qualification of a cyber operation as an attack"[56]. In this definition, a 'cyber means of warfare' includes 'cyber weapons and their associated cyber systems', including 'any cyber device, material, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyber-attack'[57].

The UN General Assembly's definition of aggression includes the use of 'any weapons' against another state. Such a broad approach leads to the conclusion that, regardless of the type of weapon used in a hostile act against a state, it can be considered an act of aggression "if the circumstances are of sufficient gravity"[58]. Hence, the differences between kinetic and cyber devices may have a limited impact on the classification of aggression (attack) for the purpose of Article 42(7) TEU and cyber operations.

Moreover, while it may be of some assistance to confront the existing definitions of 'cyber weapons' in a case of assessing the relevance of a cyber-attack to Article 42(7) TEU, the outcome of such an examination will not give legitimate and unquestionable arguments for qualifying or disqualifying

---

53 *Armed* [term], [in:] *Cambridge Dictionary*, https://dictionary.cambridge.org/dictionary/english [accessed: 10.01.2022].

54 G.H. Todd, *Armed attack in cyberspace*..., *op. cit.*, p. 80.

55 W.H. Boothby, *Weapons, Prohibited*, [in:] *Max Planck Encyclopedia of Public International Law*, 02.2015, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e447 [accessed: 19.02.2022].

56 M.N. Schmitt, *Tallin Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge 2013, p. 452.

57 S. de Tomas Colatin, A. Väljataga, *Data as a Weapon: refined Cyber Capabilities under Weapon Reviews and International Human Rights law*, NATO CCDCOE, Tallinn 2020, p. 5, https://ccdcoe.org/uploads/2020/05/Data_as_a_weapon_-_reviews_and_oversight_FINAL_PDF.pdf [accessed: 10.01.2022].

58 G.H. Todd, *Armed attack in cyberspace*..., *op. cit.*, p. 80.

actions as cyber-attacks. As pointed out by Tallin Manual, "the mere fact that a computer (rather than a more traditional weapon, weapon system, or platform) is used during an operation has no bearing on whether that operation amounts to a 'use of force' [...]"[59]. In paragraph 39 of its *Nuclear Weapons* advisory opinion, the International Court of Justice stated that both Articles 2(4) and 51 of the United Nations Charter dealing with the prohibition of the use of force and self-defence apply to "any use of force, regardless of the weapons employed"[60]. It is not the instrument used that determines whether the use of force threshold has been crossed, but rather the consequences of the operation and its surrounding circumstances[61].

Notion of a 'territory' in the context of cyber operations

A concept of territory within the meaning of Article 42(7) TEU requires a further explanation considering that it is one of the requirements for the activation of Article 42(7) TEU.

In the classical approach, it is one of the three elements of statehood (the other two being people and power). Article 52 TEU provides that the Treaties apply to all the member states of the EU. This provision is based on Article 29 of the Vienna Convention on the Law of Treaties, which states that as a principal rule "a treaty is binding upon each party in respect of its entire territory"[62]. The territory covers the area over which a party to the treaty exercises sovereignty[63]. From a geographical perspective, it embraces all that State's land, internal and territorial waters, and air space, whether or not these areas are part of the metropolitan area, though the continental shelf, the exclusive economic zone, and the fishery zones are not covered[64]. As pointed out by Blanke, functionally, the territorial scope of Union law also extends to vessels and aircrafts registered in a member state[65].

Article 355 of the TFEU further specifies that the territory of the EU includes: Guadeloupe, French Guiana, Martinique, Réunion, Saint-Barthélemy,

59 M.N. Schmitt, *Tallin Manual...*, *op. cit.*, p. 328.
60 *Ibidem*.
61 *Ibidem*.
62 H.-J. Blanke, *Article 52 – Commentary*, [in:] *Treaty on European Union*, eds H.-J. Banke, St. Miangameli, Springer Verlag, Berlin–Heidelberg 2013, p. 1434.
63 *Ibidem*.
64 *Ibidem*, p. 1435.
65 *Ibidem*, p. 1436.

Saint-Martin, the Azores, Madeira, and the Canary Islands. Furthermore, it also provides specific provisions for certain territories that are treated differently[66]. The Treaties shall apply to the European territories for whose external relations a Member State is responsible[67]. However, the five European 'microstates' (Andorra, Liechtenstein, Monaco, San Marino, and Vatican City) do not form part of the Union territory[68].

The commentaries to the Treaties do not elaborate on the meaning and application of the term 'territory' to cyberspace, and there is no commonly agreed legal definition of 'cyberspace'. There is, however, a widely held view that it "is not a physical place – it defies measurement in any physical dimension or time space continuum. It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructure, commonly referred to as the World Wide Web"[69].

Cyberspace does not have territorial (physical) boundaries, and interactions in cyberspace are of a virtual character through the transmission of data, signalling, and sending of content between physical devices. However, as pointed out by Harriet Moynihan, cyberspace includes computers, integrated circuits, cables and communication infrastructures, software logic, data packets and electronics, as well as humans. This physical equipment is located within the territory of a state and is owned by governments and companies, making a cyberspace well rooted in the physical world[70].

Cyber operations involve people in one territorial jurisdiction trading with others in another jurisdiction or engaging in activities in one jurisdiction that cause real-world effects in another territorial jurisdiction[71].

The cyber territory of a state may be linked to a citizenship of the data generator, its residence, the place of registration of the entity that processes

---

66 Compare paragraph 4 and paragraph 5 of Article 355 of the TFEU.

67 In practice, this provision applies to Gibraltar (which is reaffirmed by Declaration No. 55).

68 H.-J. Blanke, *Article 52...*, *op. cit*., p. 1436.

69 W. Heintschel von Heinegg, *Legal Implications of Territorial Sovereignty in Cyberspace*, 4th International Conference on Cyber Conflict 2012, p. 9, www.ccdcoe.org/uploads/2012/01/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf [accessed: 20.03.2022].

70 H. Moynihan, *The application of international law to state cyberattacks. Sovereignty and Non-Intervention*, Chatham House, London 2019, p. 14.

71 *Ibidem*.

the data, as well as a physical location of the servers[72]. Each of them gives rise to a number of practical and legal questions.

A state has a right to exercise its sovereign powers over cyber infrastructure in its territory, exclusively and independently, within its jurisdiction. It is a violation of sovereignty when a state (including state agents, state organs, non-state actors, and proxies if their actions can be attributed to the state) exercises cyber operations in another state's territory without consent in relation to an area over which the territorial state has the exclusive right to exercise its state powers independently. As underlined by the Permanent Court of International Justice in its 1927 Lotus Case: "a State [...] may not exercise its power in any form in the territory of another State"[73].

In case of application of Article 42(7) TEU to cyber context, the territory of the EU state shall therefore be understood not just as a physical land within the boundaries, but also as a cyber environment that falls under the sovereign powers of that EU member state.

Notion of 'attacker' and 'aggressor' in context of cyber operations *(*issue of attribution*)*

The first words of Article 42(7) TEU ("If a Member State is the victim of armed aggression on its territory [...]") do not specify 'aggressor'. As history shows, in general, attacks and/or acts of aggression are triggered by states and also by other entities, including non-state actors[74].

There is no legal definition of 'non-state actors'. In practice, the notion may encompass all those actors in international relations that are not states, including individuals and entities ranging from local to global organizations and

[72] *What is the Cyber Territory of a Country?*, Nokia Bell Labs, 18.07.2019, https://docbox.etsi.org/Workshop/2019/201906_ETSISECURITYWEEK/1806_CYBERSECURITY_POLICYACTIONS/01__CYBERSECURITY_ACT/NOKIA_Holtmanns.pdf [accessed: 28.03.2022].

[73] The case of the S.S. "Lotus", Publications of the Permanent Court of International Justice, Series A, No. 10, 7.09.1927, p. 18, www.icj-cij.org/public/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf [accessed: 15.08.2022].

[74] For a general discussion on application of Article 42(7) TEU to non-state actors see: E. Suwara, *Article 42(7) of the Treaty on European Union and Non-state Actors: issues for Consideration*, "Humanitäres Völkerrecht" 2022, Band 5, Heft 1–2, pp. 36–49.

institutions, as well as non-governmental organizations or fraternal orders[75]. Also terrorists are considered non-state actors[76].

Following the events of September 11, 2001, some scholars have argued that the content of Article 51 of the UN Charter does not provide a limitation when it comes to the term of 'aggressor'[77]. They point out that non-state actors could be considered 'aggressors', and that the states have a right of self-defence against an imminent or actual armed attack by non-state actors. They underline that, if the state from whose territory the non-state actor operates is unable or unwilling to prevent attacks, a threatened state may use armed force against the non-state actor within that territory, even without the territorial state's consent[78]. In other words, the perpetrator of the armed attack mentioned in Article 51 of the UN Charter is not necessarily identified as a state[79], although the content of the provision indicates that only the state has the right of self-defence[80]. Therefore, an armed attack can be carried out by non-state actors[81], and this can justify the exercise of the right to self-defence. This rule may apply in the cyber context. Such attackers may operate transnationally, lacking direct affiliation with a state.

However, what is important, is the transborder character of such cyber operations, as the law of self-defence does not apply to intrastate cyberattacks launched from within a state against targets in that state[82]. Cyber-attacks require actions conducted by (or attributable to) one state against another, or by an external non-state group against a state[83]. The external character of cyber-attacks may mean that they originate, or are carried out, from outside the Union, or use

[75] M. Wagner, *Non-State Actors*, [in:] *Max Planck Encyclopaedia of Public International Law*, 07.2013, p. 8, https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1445?prd=OPIL [accessed: 19.02.2022].

[76] *Ibidem*.

[77] Y. Dinstein, *War, Aggression and Self-defence*, 6th ed., Cambridge University Press, Cambridge 2017, p. 241.

[78] More on the issue: D. Bethlehem, *Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors*, "The American Journal of International Law" 2012, Vol. 106, No. 4, pp. 770–777; E Wilmshurst, *Principles of International Law on the Use of Force by States in Self-Defence*, Chatham House, London 2005; L.J. van den Herik, N.J. Schrijver, *Leiden Policy Recommendations on Counter-terrorism and International Law*, "Netherlands International Law Review" 2010, Vol. 57, Issue 3, pp. 531–550.

[79] S.D. Murphy, *Terrorism, and the Concept of "Armed Attack" in Article 51 of the UN Charter*, "Harvard International Law Journal" 2002, Vol. 43, No. 1, p. 50.

[80] Y. Dinstein, *War, Aggression..., op. cit*.

[81] *Ibidem*.

[82] M.N. Schmitt, *The use of cyber force..., op. cit.*, p. 1121.

[83] *Ibidem*.

infrastructure outside the Union, are carried out by any natural or legal person, entity, or body established or operating outside the Union, or finally are carried out with the support, at the direction, or under the control of any natural or legal person, entity, or body operating outside the Union[84].

Notion of 'armed attack' and 'armed aggression' in the context of 'cyber operations'

Based on Article 42(7) TEU, the EU member states are obliged to assist any member state if it is the victim of 'armed aggression' that occurs on its territory. Of course, ending the hostilities remains the main priority. For that purpose, it does not really matter whether an act is labelled as 'invasion', 'aggression', 'armed attack' or as 'use of force'. However, the provisions should be formulated accurately to assure a rapid and adequate response[85]. The notion of 'victim', 'aggressor' and 'territory' in the context of cyber operations has already been discussed. It is therefore time to analyse 'armed attack' and 'aggression'.

It must be noted that there are some discrepancies within the EU language versions of Article 42(7) TEU and when compared with the English wording of Article 51 of the UN Charter. There are approximately eleven EU language versions that include 'armed aggression', and twelve that apply 'armed attack' in Article 42(7) TEU[86]. Therefore, both terms require some consideration.

While it is not easy to define exactly the ambit of 'armed attack', its contours become clearer when consulting a definition of aggression (as adopted in the General Assembly Resolution in 1974)[87].

According to Article 1 of the UN General Assembly (GA) Resolution 3314, 'aggression' is "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the UN Charter of the United Nation, as set out in this Definition"[88].

---

84 Council Regulation (EU) 2019/796 of 17 May..., *op. cit*.

85 J. Klabbers, *Intervention, armed intervention, armed attack, threat to peace, act of aggression, and threat or use of force: what's the difference?*, [in:] *The Oxford Handbook*..., *op. cit*., p. 505.

86 The following EU language version of Article 42(7) TEU apply 'armed aggression': ES, EN, FR, HR, IT, LV, LT, MT, PL, RO, SK. The following apply 'armed attack': BG, CZ, DK, DE, EE, EL, FI, GA, HU, NL SE, and SI.

87 Y. Dinstein, *War, Aggression*..., *op. cit.*, p. 209.

88 UN General Assembly Resolution 3314 (XXIX) of 14 December 1974, doc. A/RES/29/3314, p. 143, https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf?OpenElement [accessed: 5.12.2021].

The definition, once agreed by the UNGA, was further examined by the International Court of Justice (ICJ) in three important cases, namely Nicaragua[89], Oil Platforms[90], and Armed Activities on the Territory of the Congo Case[91].

Since 'armed attack' is mentioned in Article 51 of the UN Charter and in some of the language versions of Article 42(7) TEU as indicated above, it requires preliminary consideration. The notion of 'attack' in international law is used in two of its bodies: *jus ad bellum* (when a state resorts to force) and *jus in bello* (international humanitarian law applicable during an armed conflict). Depending on its source, the meaning of the term 'attack' differs[92]. Although the UN Charter does not explicitly define the term, it can be underlined (on the working level), that within *jus ad bellum* 'armed attack' is an action that gives States the right to a response rising to the level of a 'use of force'[93]. As rightly pointed out by M.N. Schmitt, "all armed attacks are uses of forces, but not all uses of forces are armed attacks"[94]. Therefore, "the touchstone of an armed attack is [...] the gravity of the attack"[95].

If the term 'armed attack' is confronted with 'armed aggression' based on the definitions provided above, while considering the content of Article 3 of the UN General Assembly Resolution 3314 (XXIX) of 14 December 1974[96] (enumerating specific acts of aggression), it is tempting to conclude that the term of (armed) aggression is broader than that of (armed) attack. While all armed attacks may be considered as armed aggression, not all acts of armed aggression are armed attacks. Furthermore, most of the states during the discussions within the Fourth Special Committee on the Question of Defining Aggression agreed that there is a "cascading relationship between the terms 'use of force', 'aggression' and 'armed attack'"[97]. However, what remains

---

89 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America, International Court of Justice, ICJ Reports 1986 para 14, www.icj-cij.org/en/case/70/judgments [accessed: 30.11.2021].

90 Case concerning oil platforms..., *op. cit.*, para 161.

91 Armed Activities on the Territory of the Congo, DRC v. Uganda, International Court of Justice, ICJ Reports 2005, 168, www.icj-cij.org/en/case/116 [accessed: 30.11.2021].

92 M.N. Schmitt, *"Attack" as a Term of Art*..., *op. cit*.

93 *Ibidem*, 286.

94 *Ibidem*.

95 B. Michael, *Responding to Attacks by Non-State Actors: The Attribution Requirement of Self-Defence*, "Australian International Law Journal" 2019, Vol. 19, p. 134.

96 UN General Assembly Resolution 3314 (XXIX)..., *op. cit.*

97 T. Ruys, *Armed Attack and Article 51 of the UN Charter*, Cambridge University Press, Cambridge 2010, p. 134.

clear is that the question as to what amounts to aggression and whether aggression in the sense of Article 51 of the UN Charter is conceivable in circumstances not amounting to an armed attack – has not yet received any authoritative answer[98].

Putting the above considerations into cyber context clearly indicates that the activities in cyberspace defy many of the traditional categories and principles that govern kinetic armed attack. Yet, *jus ad bellum* does apply to certain cyber operations[99]. As mentioned earlier, not every cyber operation constitutes a cyber-attack, and not every cyber-attack is an act of armed aggression or of armed attack (remembering that while all armed attacks may be considered as armed aggression, not all acts of armed aggression might amount to an armed attack). However, all armed attacks qualify as uses of forces[100]. If cyber operations are an armed attack in the meaning of Article 51 of the UN Charter, then there is a need to consider a definition of a cyber-attack and to explain the conditions for the cyber operation to rise to the level of an armed attack, as foreseen by the UN Charter.

The term 'cyber-attack' may be defined as any action taken to undermine the functions of a computer network for a political or national security purpose[101]. An action classified as a cyber-attack may be committed either by a state or by non-state actors and does not have to constitute a violation of criminal law (as it is the case for cyber-crime)[102].

According to the International Group of Experts drafting the *Tallin Manual on the International Law Applicable to Cyber Warfare*, a cyber operation resulting in significant death of or injury to persons, or damage to or destruction of property qualifies as an armed attack[103]. Hence, "a cyber-attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons, or damage or destruction to objects"[104]. Although some of the scholars agreed that a cyber operation without causing physical injuries or damage can qualify to be an armed attack, for now it represents only

98 Y. Dinstein, *Aggression*..., *op. cit*.

99 M.N. Schmitt, *The use of cyber force*..., *op. cit.*, p. 1112.

100 *Idem*, *Tallin Manual*..., *op. cit*., p. 1119.

101 O.A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, Ju Spiegel, *The Law of Cyber-Attack*, *op. cit*., p. 828.

102 *Ibidem*, 833.

103 M.N. Schmitt, *Tallin Manual*..., *op. cit*., rule 13, para 16.

104 *Ibidem*.

lex ferenda[105]. Yet, such a cyber operation may still seriously disrupt the national economy, or interfere with critical infrastructure, dramatically affecting the daily lives of affected states.

The current EU legal framework for introducing restrictive measures may into play while considering the application of Article 42(7) TEU to cyber operations.

In recent years, the European Union has also investigated cyber-attacks over the issue of the gravity of their effects. This process led to the adoption of Council Regulation 2019/796[106] and Council Decision 2019/797 (with further amendments)[107], both providing guidance on the legal notion of cyber-attacks and their relevance to the EU. Since the Council Regulation is part of EU law, its relevant provisions may serve as a basis for further analysis of cyber-attacks in the context of Article 42(7) TEU.

Article 1 of the Council Regulation provides the definition of cyber-attacks that points towards the gravity of their effect. It refers to "cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Union[108] or its Member States"[109]. It also enumerates the examples of cyber-attacks including

[105] *Idem*, *The use of cyber force...*, *op. cit.*, p. 1121.

[106] Council Regulation (EU) 2019/796 of 17 May..., *op. cit.*

[107] Council Decision (CFSP) 2019/797 of 17 May..., *op. cit.*

[108] According to Article 1(5) of the Council Regulation (EU) 2019/796 of 17 May 2019..., *op. cit.*: Cyber-attacks constituting a threat to the Union include those carried out against its institutions, bodies, offices and agencies, its delegations to third countries or to international organisations, its common security and defence policy (CSDP) operations and missions and its special representatives.

[109] According to Article 1(4) of the Council Regulation (EU) 2019/796, Cyber-attacks constituting a threat to Member States include those affecting information systems relating to, inter alia:
(a) critical infrastructure, including submarine cables and objects launched into outer space, which is essential for the maintenance of vital functions of society, or the health, safety, security, and economic or social well-being of people;
(b) services necessary for the maintenance of essential social and/or economic activities, in particular in the sectors of: energy (electricity, oil, and gas); transport (air, rail, water, and road); banking; financial market infrastructures; health (healthcare providers, hospitals and private clinics); drinking water supply and distribution; digital infrastructure; and any other sector which is essential to the Member State concerned;
(c) critical State functions, in particular in the areas of defence, governance, and the functioning of institutions, including for public elections or the voting process, the functioning of economic and civil infrastructure, internal security, and external relations, including through diplomatic missions;
(d) the storage or processing of classified information; or

actions involving any of the following: a) access to information systems, b) information system interference, c) data interference, d) data interception, where such actions are not duly authorised by the owner or by another right holder of the system or data or part of it or are not permitted under the law of the Union or of the Member State concerned[110].

While the borderline indicating the achievement of the significant effect of a cyber-attack is not described in the law, Article 3 of the Council Regulation 2019/796 enumerates factors that need to be considered while determining its level. They include:

(a) the scope, scale, impact, or severity of disruption caused, including to economic and societal activities, essential services, critical state functions, public order or public safety;
(b) the number of natural or legal persons, entities, or bodies affected;
(c) the number of Member States concerned;
(d) the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property;
(e) the economic benefit gained by the perpetrator, for himself or for others;
(f) the amount or nature of data stolen or the scale of data breaches; or
(g) the nature of commercially sensitive data accessed[111].

As it has already been mentioned, eleven EU language versions use the term 'armed aggression' and twelve include 'armed attack' in Article 42(7) TEU. Moreover, while all armed attacks may be considered as acts of armed aggression, not all acts of armed aggression are armed attacks. These statements have direct consequences for the application of Article 42(7) TEU to cyber operations.

If cyber operations against an EU member state rise to the level of 'armed aggression' in the meaning of Article 42(7) TEU, it does not mean they amount to the 'armed attack' foreseen by Article 51 of the UN Charter. Such a situation results in the need for the further assessment of whether a given cyber operation fulfils the notion of armed attack in the meaning of Article 51 of the UN Charter. Executing the obligation foreseen in Article 42(7) TEU without such an in-depth assessment may raise doubts about the legality of the response, especially if it takes form of military aid and assistance that amounts to use of force against the attacker. This means that the use of force as a form of aid and assistance by other EU member states may constitute

(e) government emergency response teams. Council Regulation (EU) 2019/796 of 17 May 2019..., *op. cit.*

110 Art. 1(3) Council Regulation (EU) 2019/796 of 17 May 2019..., *op. cit.*

111 Art. 3 Council Regulation (EU) 2019/796 of 17 May 2019..., *op. cit.*

a breach of the prohibition of use of force foreseen by Article 2(4) of the UN Charter. Therefore, the issue of in-depth assessment remains of outmost importance, especially for those EU member states that have a term 'armed aggression' in their translation of Article 42(7) TEU[112]. The cyber operations against an EU member state that amount to 'armed attack' foreseen by Article 51 of the UN Charter do not raise such doubts, as term 'armed attack' in Article 42(7) TEU, constitutes a condition for launching aid and assistance in response to such an attack. The EU member states, prior of providing aid and assistance based on Article 42(7) TEU must conclude that that an armed attack has been mounted and that the use of force is necessary, proportionate, and meets the requirements of imminence or immediacy[113].

Conclusion

The research undertaken in this publication focused on attempting to respond to two main questions: whether Article 42(7) TEU applies to cyber operations, and if so, when a cyber operation rises to the level of an 'armed aggression' in the meaning of Article 42(7) TEU.

While the EU member state exercises the right of self-defence provided in Article 51 of the UN, in case of armed aggression of the EU territory and based on Article 42(7) TEU, the other EU member states have obligation to aid and assist it in all the means in their power. It is UN Charter that gives – under certain conditions – the right of exercising the self-defence and permission to use of force against armed attack to the affected state. The role of Article 42(7) TEU is, in that sense, complementary to the UN Charter, as it only stipulates the obligation of other EU member states, once the occurrence of 'armed attack' has been verified. It is against the provisions of the UN Charter that the fulfilment of criteria for 'armed attack' needs to be checked by the EU member states concerned.

Although there is no commonly agreed definition of victim in international law, literally it means 'one that is acted on and usually adversely affected by a force or agent'. Being already a victim, as stipulated in Article 42(7) TEU, leads to the assumption that the act(s) of the aggression has occurred, or it is ongoing, adversely affecting EU member state. It may exclude the relevance

[112] In other words: while applying Article 42(7) TEU, in case of cyber incident(s), an EU member state will likely refer to its content using its own language version of the provision. Reference to 'armed aggression', while describing the incident may constitute insufficient grounds for application of Article 51 of the UN Charter.

[113] M.N. Schmitt, *The use of cyber force*..., *op. cit.*, p. 1128.

and application of anticipatory and pre-emptive self-defence when the status of an affected state does not necessarily qualify under such a category. It could be agreed, that if an armed attack or aggression has not occurred, then the state cannot yet be considered 'a victim' of it. In pre-emptive and anticipatory self-defence the affected state does not yet have a status of a victim. In the case of cyber operations, it may happen that the affected state is not aware it is under attack. In such a case, its right to respond in self-defence will only persist if the attacks are likely to continue.

The weapon used does not impact a classification of cyber operation as 'an armed aggression' in the meaning of Article 42(7) TEU or as 'armed attack' in the meaning of Article 51 of the UN Charter. Cyber operations amounting to acts of armed attack do not necessarily make direct use of any kinetic weapons. It is not the instrument used but rather the consequences of the operation and its surrounding circumstances that are important for assessment of the occurrence of the armed attack in the cyber context.

Defining the EU territory in cyberspace is challenging as it requires the analysis of attribution linked to location of, i.e., persons and equipment, all traceable physical elements that are involved in a cyber operation. This analysis is important for attributing a given cyber operation to aggressor or attacker. An EU member state has sovereign power over cyber territory and armed aggression within the meaning of Article 42(7) TEU violates this sovereign right.

Cyber operations amounting to armed attack in the meaning of Article 51 of the UN Charter may be conducted by one state against another or by an external non-state group against a state. The transborder elements of such operations is crucial, as intrastate cyber-attacks do not allow to the exercise of the right of self-defence.

To conclude, to trigger application of Article 42(7) TEU, cyber operations must be assessed against a notion of 'armed attack' in the meaning of Article 51 of the UN Charter. The cyber operation can be considered an armed attack in the meaning of Article 51 of the UN Charter, if it results in significant death of or injury to persons, or damage to or destruction of property. Lack of physical effect may constitute grounds not to be considered as 'armed attack' in the meaning of Article 51 of the UN Charter. Assessing a cyber operation as an 'armed aggression' although may give grounds to activate Article 42(7) TEU but may not fulfil the requirement provided in Article 51 UN Charter. In such cases, the UN Security Council, based on Article 39 of the UN Charter, has authority to determine the existence of any threat to the peace, breach of the peace, or act of aggression. However, it may not go unnoticed that, so far, no cyber operation has ever been characterized by the

Security Council as meeting the Article 39 criteria[114]. It is of utmost importance that the EU member states, prior of providing aid and assistance based on Article 42(7) TEU in the case of a cyber operation, conclude that an armed attack has been mounted and that the use of force is necessary, proportionate, and meets the requirements of imminence or immediacy.

References

Literature

An object [term], [in:] *Merriam-Webster Dictionary*, www.merriam-webster.com/dictionary [accessed: 10.02.2022].

Armed [term], [in:] *Cambridge Dictionary*, https://dictionary.cambridge.org/dictionary/english [accessed: 10.01.2022].

Bethlehem D., *Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors*, "The American Journal of International Law" 2012, Vol. 106, No. 4, pp. 770–777.

Blanke H.-J., *Article 52 – Commentary*, [in:] *Treaty on European Union*, eds H.-J. Banke, St. Miangameli, Springer Verlag, Berlin–Heidelberg 2013.

Boothby W.H., *Weapons, Prohibited*, [in:] *Max Planck Encyclopedia of Public International Law*, 02.2015, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e447 [accessed: 19.02.2022].

Brownlie I., *International law, and the Use of Force by States*, Clarendon Press, Oxford 1963.

De Casadevante Romani C.F., *International Law of Victims*, "Max Planck Yearbook of United Nations Law" 2010, Vol. 14, pp. 219–272.

De Tomas Colatin S., Väljataga A., *Data as a Weapon: refined Cyber Capabilities under Weapon Reviews and International Human Rights law*, NATO CCDCOE Tallinn 2020, https://ccdcoe.org/uploads/2020/05/Data_as_a_weapon_-_reviews_and_oversight_FINAL_PDF.pdf [accessed: 10.01.2022].

Dinstein Y., *Aggression* [term], [in:] *Max Planck Encyclopedia of Public International Law*, 09.2015, https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e236 [accessed: 11.02.2022].

Dinstein Y., *War, Aggression and Self-defence*, 6th ed., Cambridge University Press, Cambridge 2017.

Dubuisson F., Lagerwall A., *The threat of the use of force and ultimate*, [in:] *The Oxford Handbook of the Use of Force in International Law*, ed. M. Weller, Oxford University Press, Oxford 2017.

European Civil Protection and Humanitarian Aid Operations, European Commission, https://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en [accessed: 10.01.2022].

Hathaway O.A., Crootof R., Levitz P., Nix H., Nowlan A., Perdue W., Spiegel J., *The Law of Cyber-Attack*, "California Law Review" 2012, Vol. 100, No. 4, pp. 817–886.

Heintschel von Heinegg W., *Legal Implications of Territorial Sovereignty in Cyberspace*, 4th International Conference on Cyber Conflict 2012, www.ccdcoe.org/

[114] *Ibidem*, p. 1117.

uploads/2012/01/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf [accessed: 20.03.2022].

How does the Integrated Political Crisis Response (IPCR) mechanism work?, Council of the EU, 2018, www.consilium.europa.eu/media/45843/ipcr-mechanism.pdf [accessed: 10.01.2022].

Jessup P., *A Modern law of Nations*, Archon Books, Hamden CT 1968.

Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade, High Representative of the Union for Foreign Affairs and Security Policy, 16.12.2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&rid=8 [accessed: 1.06.2022].

Michael B., *Responding to Attacks by Non-State Actors: The Attribution Requirement of Self-Defence*, "Australian International Law Journal" 2019, Vol. 19, pp. 133–159.

Moynihan H., *The application of international law to state cyberattacks. Sovereignty and Non-Intervention*, Chatham House, London 2019.

Murphy S.D., *Terrorism, and the Concept of "Armed Attack" in Article 51 of the UN Charter*, "Harvard International Law Journal" 2002, Vol. 43, No. 1, pp. 41–51.

Mutual defence clause (Article 42.7 TEU), European Parliament, www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede200612mutualdefsolidarityclauses_/sede200612mutualdefsolidarityclauses_en.pdf [accessed: 15.12.2021].

New EU Cybersecurity Strategy, and new rules to make physical and digital critical entities more resilient, European Commission, 16.12.2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391 [accessed: 1.02.2022].

Pawlak P., *Cybersecurity and Cyberdefence EU Solidarity and Mutual Defence Clauses*, 06.2015, www.europarl.europa.eu/RegData/etudes/BRIE/2015/559488/EPRS_BRI(2015)559488_EN.pdf [accessed: 15.12.2021].

Randelzhofer A., [in:] *The UN Charter of the United Nations, a commentary*, eds B. Simma, D.-E. Khan, G. Nolte, A. Paulus, N. Wessendorf, 3th ed., Vol. 1, Oxford University Press, Oxford–New York 2012.

Rehrl J., *Invoking the EU's Mutual Assistance Clause. What it says, what it means*, Egmont Institute, 20.11.2015, www.egmontinstitute.be/invoking-the-eus-mutual-assistance-clause-what-it-says-what-it-means [accessed: 14.01.2022].

Ruys T., *Armed Attack and Article 51 of the UN Charter*, Cambridge University Press, Cambridge 2010.

Sari A., *The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats*, "Harvard National Security Journal" 2019, Vol. 19, pp. 405–460.

Schinas M., *Keynote speech of the European Commission Vice President*, 17.02.2022, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_1163 [accessed: 20.02.2022].

Schmitt M.N., *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, [in:] *4th International Conference on Cyber Conflict*, eds C. Czosseck, R. Ottis, K. Ziolkowski, NATO CCDCOE Publication, Tallin 2012, pp. 283–293.

Schmitt M.N., *Tallin Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013.

Schmitt M.N., *The use of cyber force and international law*, [in:] *The Oxford Handbook of the Use of Force in International Law*, ed. M. Weller, Oxford University Press, Oxford 2017, pp. 1110–1130.

Shah N.A., *Self-defence Anticipatory Self-defence, and Pre-emption: International Law's Response to Terrorism*, "Journal of Conflict and Security Law" 2017, Vol. 12, Issue 1, pp. 95–126.

Significant cyber incidents since 2006, Center for Strategic and International Studies, https://csis-website-prod.s3.amazonaws.com/s3fs-public/220805_Significant_Cyber_Events_0.pdf?ruYyPiNzwADjystZd.g9QgMEPY1K28Et [accessed: 29.08.2022].

Suwara E., *Article 42(7) of the Treaty on European Union and Non-state Actors: issues for Consideration*, "Humanitäres Völkerrecht" 2022, Band 5, Heft 1–2, pp. 36–49.

Suwara E., *Klauzula wzajemnej pomocy i wsparcia zawarta w art. 42 ust. 7 Traktatu o Unii Europejskiej*, "Państwo i Prawo" 2018, nr 7, pp. 91–107.

Threat [term], [in:] *Merriam-Webster Dictionary*, www.merriam-webster.com/dictionary [accessed: 11.02.2022].

Todd G.H., *Armed attack in cyberspace: deterring asymmetric warfare with an asymmetric definition*, "The Air Force Law Review" 2009, Vol. 19, pp. 65–102.

Upeniece V., *Conditions for the legal commencement of an armed attack*, [in:] *6th International Interdisciplinary Scientific Conference Society. Health. Welfare. 23–25 November 2016, Riga*, ed. U. Berkis *et al.*, EDP Sciences, 2018, pp. 1–7.

Van den Herik L.J., N.J. Schrijver, *Leiden Policy Recommendations on Counter-terrorism and International Law*, "Netherlands International Law Review" 2010, Vol. 57, Issue 3, pp. 531–550.

Victim [term], [in:] *Merriam-Webster Dictionary*, www.merriam-webster.com/dictionary [accessed: 10.02.2022].

Wagner M., *Non-State Actors*, [in:] *Max Planck Encyclopaedia of Public International Law*, 07.2013, https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1445?prd=OPIL [accessed: 19.02.2022].

What is the Cyber Territory of a Country?, Nokia Bell Labs, 18.07.2019, https://docbox.etsi.org/Workshop/2019/201906_ETSISECURITYWEEK/1806_CYBERSECURITY_POLICYACTIONS/01__CYBERSECURITY_ACT/NOKIA_Holtmanns.pdf [accessed: 28.03.2022].

Wilmshurst E., *Principles of International Law on the Use of Force by States in Self-Defence*, Chatham House, London 2005.

Acts of law and judgments

Armed Activities on the Territory of the Congo, DRC v. Uganda, International Court of Justice, ICJ Reports 2005, 168, www.icj-cij.org/en/case/116 [accessed: 30.11.2021].

Article 2(4), https://legal.un.org/repertory/art2/english/rep_supp7_vol1_art2_4.pdf [accessed: 13.01.2022].

Case concerning oil platforms Islamic Republic of Iran v. United States of America, International Court of Justice, ICJ Reports 2003, para. 161, https://www.icj-cij.org/en/case/90 [accessed: 30.11.2021].

Consolidated Version of the Treaty on European Union [2007], OJ. C. 326., 26.10.2012, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT [accessed: 15.12.2021].

Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, Official Journal L 129I, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2019:129I:FULL&from=EN [accessed: 20.02.2022].

Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, Official Journal L 129I, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2019:129I:FULL&from=EN [accessed: 20.02.2022].

Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), Document 9916/17, General Secretariat of the Council, 7.06.2017, https://ccdcoe.org/uploads/2018/11/EU-170607-CyberDiplomacyToolbox-1.pdf [accessed: 13.06.2022].

Draft Directive of the European Parliament and of the Council on the resilience of critical entities, COM/2020/829, European Commission, 16.12.2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN [accessed: 1.02.2022].

Draft Directive of the European Parliament, and the Council on measures for high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, European Commission, 16.12.2020, https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union [accessed: 1.02.2022].

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), International Court of Justice, ICJ Reports 1986, www.icj-cij.org/en/case/70/judgments [accessed: 30.11.2021].

North Atlantic Treaty, Washington D.C. 4.04.1949, www.nato.int/cps/en/natolive/official_texts_17120.htm [accessed: 13.12.2021].

Protocol on the concerns of the Irish people on the Treaty of Lisbon, Official Journal of the European Union L 60/131, 2.03.2003, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2013_060_R_0129_01&rid=3 [accessed: 13.01.2022].

Resolution on the mutual defence clause (Article 42(7) TEU), 2015/3034(RSP), European Parliament, 21.01.2016, www.europarl.europa.eu/doceo/document/TA-8-2016-0019_EN.pdf [accessed: 15.12.2021].

The case of the S.S. "Lotus", Publications of the Permanent Court of International Justice, Series A, No. 10, 7.09.1927, www.icj-cij.org/public/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf [accessed: 15.08.2022].

UN General Assembly Resolution 3314 (XXIX) of 14 December 1974, doc. A/RES/29/3314, www.un.org/ga/search/view_doc.asp?symbol=A/RES/3314(XXIX) [accessed: 5.12.2021].

Cyber operations and Article 42.7 of the Treaty on European Union

The threat posed by the occurrence of cyber-attacks constitutes a challenge to national security. Such attacks may target and disturb the daily functioning of any state. Faced with complex and diverse crises, the European Union (EU) has improved its response capacities over the last decades, introducing a so-called 'aid and assistance clause' into Article 42(7) of the Treaty on European Union (TEU) applicable in the case of armed aggression against an EU member state on its territory. The main objective of this publication is to examine potential conditions for the application of Article 42(7) TEU in response to cyber operations. The author argues that under certain conditions, the aid and assistance clause in Article 42(7) TEU may be invoked in response to certain cyber operations against an EU member state on its territory.
Key words: cyber-attack, cyber operations, armed aggression, armed attack, aid and assistance clause, Article 42(7) TEU, Article 51 of the UN Charter

Operacje cybernetyczne a art. 42.7 Traktatu o Unii Europejskiej

Zagrożenia wynikające z dokonywania cyberataków stanowią wyzwanie dla bezpieczeństwa narodowego. Takie ataki mogą być wymierzone w każde państwo, aby zakłócić jego codzienne funkcjonowanie. W obliczu złożonych i różnorodnych kryzysów Unia Europejska w ostatnich dekadach zwiększyła swoje możliwości reagowania, wprowadzając do art. 42 ust. 7 Traktatu o Unii Europejskiej (TUE) tzw. klauzulę pomocy i wsparcia, mającą zastosowanie w przypadku zbrojnej agresji przeciwko państwu członkowskiemu UE na jego terytorium. Głównym celem niniejszej publikacji jest analiza potencjalnych warunków zastosowania art. 42 ust. 7 TUE w odpowiedzi na operacje cybernetyczne. Autor argumentuje, że w określonych sytuacjach klauzula pomocy i wsparcia z art. 42 ust. 7 TUE może być stosowana w odpowiedzi na niektóre operacje cybernetyczne przeciwko państwu członkowskiemu UE na jego terytorium.
Słowa kluczowe: cyberatak, operacje cybernetyczne, agresja zbrojna, atak zbrojny, klauzula pomocy i wsparcia, art. 42 ust. 7 TUE, art. 51 Karty Narodów Zjednoczonych