ROYAL HIGHER INSTITUTE
150-year think tank for DEFENCE

e-Note 40 - 11 May 2022

CENTRE for SECURITY and DEFENCE STUDIES
SECURITY & DEFENCE

Does the mutual assistance clause of the Treaty on European Union (Article 42(7) TEU) allow for an adequate response to new threats?

Estelle HOORICKX & Carolyn MOSER[1]

This e-Note is based on personal analyses presented by the authors at the European Parliament's Subcommittee on Security and Defence (SEDE) on 29 November 2021[2].

For the past two decades, European Union (EU) Member States have shown their willingness to strengthen European defence capabilities. One key element in this respect is the mutual assistance clause, as enshrined in Article 42(7) of the Treaty on European Union (TEU) since 2009. Following the Russian invasion of Ukraine in February 2022, the debate on the use of this mutual assistance clause has gained an added momentum, especially because this clause is one of the power instruments the EU wishes to capitalise on in order to deal with current threats. While having been invoked for the first and only time by France in 2015, the use of this clause still raises questions. This note therefore analyses how European Member States can operate within the framework of the mutual assistance clause with a view to dealing with "new" threats, whether they are hybrid, of a cyber nature or whether they apply emerging technologies on the various fields of confrontation (land, sea, air, space and cyber). Even though triggering the clause is no easy thing, Article 42(7) TEU provides a valuable legal basis for a collective response to cyberattacks and hybrid threats, provided that they are considered armed attacks[3]*in the legal sense of the term.*

The invasion of Ukraine reinvigorates the debate on the mutual assistance clause

At the Versailles Summit of 10 and 11 March 2022, the European Heads of State or Government stated that the Russian invasion of Ukraine constitutes "a tectonic shift in European

[1] Estelle HOORICKX (Royal Higher Institute for Defence) and Carolyn MOSER (Max Planck Institute for Comparative Public Law and International Law). E-Note translated from French by Claire Nardon (Department Productions, Public Relations and Support, RHID).

[2] The hearing covered the applicability of the mutual assistance clause of the Treaty on European Union (Article 42(7) TEU) in order to deal with new threats, including cyberattacks, hybrid threats or attacks using new and emerging technologies (www.europarl.europa.eu/cmsdata/242774/Programme_SEDE_Hearing_MutualDefenceClause_29112021.pdf).

[3] The French version of the Treaty on European Union (TEU) stipulation uses the term "*agression armée*", as does the French version of Article 51 of the UN Charter.

history"[4]. The Member States have therefore committed themselves to substantially strengthening their defence capabilities by 2030 and to placing greater emphasis on countering "ever-growing hybrid warfare" and on fighting disinformation[5]. They also recalled that the "solidarity between Member States is reflected in Article 42(7) TEU [Treaty on European Union]"[6]. Moreover, this mutual assistance clause[7] is at the heart of the Strategic Compass adopted by the Council of the European Union on 21 March 2022[8]. This document states that the new strategic landscape "requires [the Member States] to act with a far greater sense of urgency and determination and show mutual assistance and solidarity in case of aggression against one of us"[9]. This acknowledgement is particularly relevant considering the current geopolitical context in which increasingly complex threats are taking on unprecedented proportions[10]. Furthermore, mutual assistance in case of aggression is fundamental in order to strengthen the EU's strategic and decision-making autonomy.

The use of the mutual assistance clause codified by Article 42(7) TEU and invoked for the first (and only) time by France in November 2015 after the Paris attacks, still raises questions[11]. Since the clause includes obligations that are rather vague and not specified by other European legal or political sources, its implementation modalities remain unclear. In fact, it is up to the Member States providing aid and assistance to define the military and civilian assets they wish to deploy for the sake of collective self-defence. Countries providing support thus have considerable decision-making and operational leeway[12]. As a result, the Member States only provided a modest, or even symbolic, response to France's call for aid and assistance in 2015 and prevented the French army from reducing its presence during its extraterritorial counter-terrorism missions, as desired by France[13].

Nevertheless, for EU Member States that are not members of NATO, such as Finland and Sweden in particular[14], which cannot (currently)[15] rely on Article 5 of the North Atlantic Treaty

[4] European Council, "Informal meeting of the Heads of State or Government – Versailles Declaration, 10 and 11 March 2022", March 11, 2022, 3, https://www.consilium.europa.eu/media/54773/20220311-versailles-declaration-en.pdf.

[5] European Council, "Versailles Declaration", 4.

[6] European Council, "Versailles Declaration", 3.

[7] While this article has often been referred to as "mutual defence clause", the doctrine generally prefers the generic term "mutual assistance clause". See for example Mattias Fischer and Daniel Thym, "Article 42 [CSDP: Goals and Objectives; Mutual Defence]", in *The Treaty on European Union (TEU). A Commentary*, edited by Hermann-Josef Blanke and Stelio Mangiameli (Berlin; Heidelberg: Springer, 2013); Panos Koutrakos, *The EU Common Security and Defence Policy*, EU law library (Oxford; New York: Oxford University Press, 2013), 68–71. Furthermore, jurists of the Council of the EU, who have written a confidential note on this topic in July 2016, tend to consider Article 42(7) TEU as a mutual *assistance* clause, rather than a mutual *defence* clause within the meaning of NATO's Article 5 (André Dumoulin and Nicolas Gros-Verheyde, *La politique européenne de sécurité et de défense commune* (Brussels: Éditions du Villard, 2017), 324).

[8] Council of the European Union, *A Strategic Compass for Security and Defence: For a European Union that Protects its Citizens, Values and Interests and Contributes to International Peace and Security*, document of the Council no. 7371/22, March 21, 2022.

[9] Council of the European Union, "Strategic Compass" (2022), 12.

[10] In this regard, see the annual report of the European Parliament on the implementation of the Common Security and Defence Policy (2021) (https://www.europarl.europa.eu/doceo/document/TA-9-2022-0040_EN.html).

[11] Nicolas Gros-Verheyde, "À défaut d'article 5 de l'OTAN peut-on utiliser l'article 42-7 de l'UE ? Faut-il l'encadrer ?", *B2 Le quotidien de l'Europe géopolitique*, October 10, 2021, https://club.bruxelles2.eu/2021/10/a-defaut-darticle-5-de-lotan-peut-on-utiliser-larticle-42-7-de-lue-faut-il-lencadrer/.

[12] Koutrakos, *The EU Common Security and Defence Policy*, 69; Carolyn Moser, "Awakening dormant law – or the invocation of the European mutual assistance clause after the Paris attacks", *Verfassungsblog,* November 18, 2015, http://verfassungsblog.de/awakening-dormant-law-or-the-invocation-of-the-european-mutual-assistance-clause-after-the-paris-attacks/.

[13] Dumoulin and Gros-Verheyde, *La politique européenne de sécurité et de défense commune,* 331.

[14] Six out of 27 EU Member States are not NATO members, namely Sweden, Finland, Austria, Cyprus, Ireland and Malta.

[15] The recent Russian invasion of Ukraine has accelerated the debate on a possible accession of Finland and Sweden to NATO. In the next coming days, both countries are likely to officially hand in their applications to join NATO. Before their membership is ratified, both countries' security will hinge on the security assurances given by the NATO members. Triggering Article 42(7) but also bilateral support from the United States are some of the options being considered (for more

enshrining the principle of collective defence, the EU mutual assistance clause is a particularly important tool for ensuring their security[16]. Indeed, the clause is based on the obligation for all Member States to provide aid and assistance "[i]f a Member State is a victim of armed aggression on its territory". However, at present, neither in theory nor in practice is Article 42(7) TEU equivalent to NATO's Article 5[17]. On the one hand, the Member States are not willing to create an alternative military alliance to NATO; on the other hand, the EU (currently) does not have sufficient military assets to act autonomously[18]. Hence, even if the shock caused by the Russian attack has pressed European countries to take a historic step – i.e. supplying and financing lethal and non-lethal weapons to support Ukraine[19] –, the Member States express differing views on the subsidiary or complementary nature of European defence with regard to NATO commitments, as testified by the fuzzy language used in the Strategic Compass when referring to Article 42(7) TEU and its link with NATO's collective defence.

Furthermore, Western allies fear that Moscow will ramp up its cyberattacks and disinformation campaigns against the 27 EU countries that have adopted sanctions against Russia and/or provide besieged Ukraine with military equipment[20], including within the framework of the European Peace Facility[21]. In this context, the suspension of broadcasting in the European Union of the Russian media outlets *Sputnik* and *Russia Today* aims to fight disinformation and information manipulation campaigns against the EU and its Member States[22]. Cyberattacks can indeed be very effective in terms of sabotage, espionage and subversion on a large scale, but it can also have serious consequences for infrastructure, the economy, health care systems and democratic processes in Europe[23].

This note therefore intends to analyse how EU Member States can operate within the framework of the mutual assistance clause established in Article 42(7) TEU in order to deal with new threats, whether they are hybrid, of a cyber nature or whether they apply emerging technologies. It also aims to examine in more depth the legal implications of invoking this clause under European and

information on this topic, read: Aurélie Pugnet, "Adhésion de la Finlande et Suède à l'OTAN: des garanties de sécurité à trouver", *B2 Le quotidien de l'Europe géopolitique*, April 7, 2022, https://club.bruxelles2.eu/2022/04/analyse-adhesion-de-la-finlande-et-suede-a-lotan-des-garanties-de-securite-a-trouver/; Anne-Françoise Hivert, "La Finlande fait un premier pas vers une candidature à l'OTAN", *Le Monde*, April 14, 2022, https://www.lemonde.fr/international/article/2022/04/14/la-finlande-fait-un-premier-pas-vers-une-candidature-a-l-otan_6122066_3210.html).

[16] This is particularly evidenced by a letter from the Finnish and Swedish Prime Ministers Sanna Marin and Magdalena Andersson, which has been sent to the President of the European Council Charles Michel ahead of the meeting of Heads of State or Government in Versailles, emphasising the importance of the EU mutual assistance clause. For more information: https://valtioneuvosto.fi/en/-/10616/prime-ministers-of-finland-and-sweden-stress-role-of-eu-as-security-provider.

[17] Koutrakos, *The EU Common Security and Defence Policy*, 68–71.

[18] Nicolas Gros-Verheyde, "À défaut d'article 5 de l'OTAN peut-on utiliser l'article 42-7 de l'UE ? Faut-il l'encadrer ?", *B2 Le quotidien de l'Europe géopolitique*, October 8, 2021, https://club.bruxelles2.eu/2021/10/a-defaut-darticle-5-de-lotan-peut-on-utiliser-larticle-42-7-de-lue-faut-il-lencadrer/; Philippe Gélie, "Charles Michel : 'L'UE vit un moment copernicien sur la défense'", *Le Figaro*, March 13, 2022, https://www.lefigaro.fr/international/charles-michel-l-ue-vit-un-moment-copernicien-sur-la-defense-20220313.

[19] The Council made its first decisions on this matter on 28 February. See: Council Decision (CFSP) 2022/338 of 28 February 2022 on an assistance measure under the European Peace Facility for the supply to the Ukrainian Armed Forces of military equipment, and platforms, designed to deliver lethal force (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022D0338); Council Decision (CFSP) 2022/339 of 28 February 2022 on an assistance measure under the European Peace Facility to support the Ukrainian Armed Forces (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2022:061:FULL&from=EN).

[20] Sue Halpern, "The Threat of Russian Cyberattacks looms large", *The New Yorker*, March 22, 2022, https://www.newyorker.com/news/daily-comment/the-threat-of-russian-cyberattacks-looms-large.

[21] See Council Decisions mentioned above (note 19).

[22] Council Decision (CFSP) 2022/351 of 1 March 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. RT France's request for interim relief has been rejected by order of the president of the General Court of the EU of 30 March 2022 (T-125/22 R), meaning that the restrictive measures against Russian media remain in place.

[23] Council of the European Union, "Strategic Compass" (2022), 22.

international law. Before looking into the new threats as well as their strategic and legal characteristics, it is important to recall the content of the mutual assistance clause and the related right to self-defence.

Article 42(7) TEU, or enshrining collective self-defence

Article 42(7) TEU enshrines the right of collective self-defence, which reads as follows:

> *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.*

Self-defence is a crucial element of international law, enabling states to protect and defend their sovereignty. Self-defence, as set out in Article 51 of the Charter of the United Nations (hereafter referred to as "the Charter"), is indeed a main exception to the prohibition of the use of force as imposed by Article 2(4) of the Charter[24]. It is one of the most controversial legal issues, not only due to the constantly evolving security environment, but also because some states invoke the right of self-defence to give an aura of legitimacy to their use of force that is not necessarily legal[25]. In any event, although traditionally applied to two states, self-defence is now increasingly being used in a collective context, including in order to counter attacks by non-state actors[26].

Despite the uncertainties – not to say ambiguities – about the notion of self-defence, there is consensus that five criteria deriving from the practice of states and international jurisprudence must be met to invoke it[27]. First, resorting to self-defence is only permitted if an armed attack occurs, which can be defined as a large-scale border incident, followed by a particular impact, which may be caused by a single act or a series of minor attacks. If the threshold of an armed attack has not been reached, states cannot legally resort to force, but will rather be limited to retaliatory sanctions[28] or

[24] Christopher Greenwood, "Self-Defence » in *Max Planck Encyclopedia of Public International Law* (Oxford, New York: Oxford University Press, 2012 [last updated in 2021]), para. 1.

[25] Russia, for example, tries to justify its recent invasion of Ukraine (more precisely, the Ukrainian Donetsk and Luhansk oblasts) by claiming that the use of force on Ukrainian territory complies with the right of self-defence. For more information on this topic, see the letter dated 24 February 2022 from the Permanent Representative of the Russian Federation to the United Nations in accordance with Article 51 of the Charter (circulated as document S/2022/154).

[26] See the academic discussion on this matter in Greenwood, "Self-Defence", para. 19 and Karl Zemanek, "Armed Attack" in *Max Planck Encyclopedia of Public International Law* (Oxford, New York: Oxford University Press, 2012 [last updated in 2013]).

[27] A key case-law reference in this regard is the judgment of the International Court of Justice (on the merits) in *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* of 27 June 1986. For an exhaustive analysis of these criteria, see Greenwood, "Self-Defence", paras. 7-51.

[28] A retaliatory measure is defined as "une mesure inamicale, licite en elle-même, prise par un [État], en riposte à un comportement inamical d'un autre [État], que ce comportement soit ou non licite"[free translation: "an unfriendly measure, lawful in itself, taken by a [state] in response to unfriendly conduct of another [state], whether or not such conduct is lawful"]. See Jean Salmon (red.), Dictionnaire de Droit international public (Bruxelles : Bruylant, 2001), 1007.

countermeasures[29], including economic or financial sanctions, or individual restrictive measures such as freezing assets and restrictions on access to the territory. Second, self-defence must be necessary and proportionate. Third, an attack must have occurred, be ongoing or imminent[30] in order for the attacked state to be entitled to invoke self-defence[31]. Fourth, every United Nations Member State shall immediately report any self-defence measures to the United Nations Security Council pursuant to Article 51 of the Charter. The same requirement applies to states deciding to support a country under attack in the context of collective self-defence. Fifth, under international law, the act of resorting to self-defence can take place both within and outside the territory of the attacked country[32].

Article 42(7) TEU embeds any collective response by EU Member States to an armed attack on one of the Member States into this international legal framework[33]. On the one hand, the clause specifies that EU collective self-defence must be in accordance with Article 51 of the Charter. This means, amongst others, that once the clause is triggered, the state invoking it and the Member States that are coming to the aid of the attacked country shall give notification thereof to the Security Council. The implementation of the clause must furthermore be consistent with the Member States' commitments under NATO. Finally, the act of resorting to collective self-defence may take place outside the EU territory. This latter element is one of the main reasons why France decided in 2015 to activate Article 42(7) TEU rather than Article 222 TFEU (Treaty on the Functioning of the European Union) relating to terrorist attacks, or natural or man-made disasters that might hit an EU country, as it only provides international assistance on the Member States' territories[34]. In contrast, by invoking the clause of Article 42(7), France was able to maintain control over its sovereignty, and notably over its foreign policy, while at the same time strengthening Europe's commitment to international anti-terrorist operations and, in so doing, allowing for reduced French-led operations[35].

[29] Countermeasures are "des mesures prises par un État en vue de faire respecter et de protéger ses intérêts au cas où ceux-ci seraient lésés par un autre État" [free translation : " countermeasures are measures taken by a State in order to protect its interests against any wrongful acts by another State"]. See Jean Salmon (dir.), Dictionnaire de Droit international public (Bruxelles: Bruylant, 2001), 259-260. For further legal details on countermeasures, see Federica Paddeau, "Countermeasures", in *Max Planck Encyclopedia of Public International Law* (Oxford, New York: Oxford University Press, 2012 [last updated in 2015]).

[30] For a country like Israel, for example, the imminence of an armed attack can also be a criterion for resorting to self-defence. This is referred to as "preventive" self-defence, i.e. self-defence based on the probability of a "threat" becoming an actual attack. However, this conception of self-defence is recognised neither by NATO nor by the EU (Greenwood, "Self-Defence"; Michael Wood, "International Law and the use of force: What happens in practice?"*, Indiana Journal of International Law* 53, 2013).

[31] For more information on the temporal dimension of self-defence, see Greenwood, "Self-Defence", paras. 41-51 and Wood, "International Law and the use of force: What happens in practice?".

[32] This territorial flexibility extends to collective self-defence, as demonstrated by the (recent) practice of states, for instance.

[33] Moser, "Awakening dormant law".

[34] Article 222 of the Treaty on the Functioning of the European Union stipulates that "[t]he Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States, to […] assist a Member State in its territory, at the request of its political authorities" (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12016E222&from=FR).

[35] Moser, "Awakening dormant law"; Estelle Hoorickx, "Countering 'Hybrid Threats': Belgium and the Euro-Atlantic Strategy", *Security & Strategy* 131, October 2017, 39-40, https://www.defence-institute.be/wp-content/uploads/2020/03/ss-131-en.pdf.

Relatively flexible implementation of the mutual assistance clause

After triggering Article 42(7) TEU, the Member States are obliged to provide support. Indeed, the clause includes an obligation that is not merely symbolic, even though it cannot be enforced by a judicial body[36]. A series of somewhat vague criteria nevertheless enable Member States to reduce the binding nature of their duty of aid and assistance[37]. It is for each Member State to determine at its total discretion the nature of aid and assistance it wishes to provide to an attacked country[38], including deploying military assets, but also offering economic assistance, diplomatic support, logistic aid, personnel or exchanging intelligence information[39]. The attacked country having invoked the clause is tasked with coordinating these different kinds of support: it coordinates, bilaterally, with the other states the measures to be taken in response to the attack.

As the clause contains an interstate obligation, no mention is made of EU institutions – neither as a victim of a possible armed attack nor as the actor implementing this clause. It can, however, be assumed that if an EU institution were to fall victim to an armed attack, the host state would trigger the clause in its place. It should then decide either to implement this measure bilaterally – with the host state taking the lead and liaising with the other Member States – or to entrust an EU body or institution with this task[40]. Conversely, the Strategic Compass advocates that the EU Military Staff (EUMS) plays a role in implementing Article 42(7) TEU, but only if requested by the Member States[41].

The difficulty of applying Article 42(7) TEU in case of "ambiguous warfare"[42]

As explained above, the mutual assistance clause can only be triggered if an armed attack occurs. However, it is not always easy to know whether the new ways of waging war, such as cyberattacks or disinformation campaigns, can be classified as an attack of this type.

"New threats" – whether they are cyberattacks or hybrid campaigns – share a number of fundamental characteristics, namely both their coercive and subversive nature, their use by state and non-state actors[43], and their main objective to exploit the weaknesses of the intended target while creating ambiguity so as to avoid suffering the consequences of a political, military (including cyber) and/or legal reaction of the international community[44]. The perpetrators of a hybrid attack will thus, as far as possible, use modi operandi – such as cyberattacks, disinformation campaigns or proxy wars –

[36] Dumoulin and Gros-Verheyde, *La politique européenne de sécurité et de défense commune*, 328.
[37] Moser, "Awakening dormant law".
[38] Senate (France), Information Report no. 626(2018-2019) of Mr Ronan Le Gleut and Ms Hélène Conway-Mouret, on behalf of the French Committee on Foreign Affairs, Defence and Armed Forces, submitted on 3 July 2019 (https://www.senat.fr/rap/r18-626-1/r18-626-14.html).
[39] Dumoulin and Gros-Verheyde, *La politique européenne de sécurité et de défense commune*, 327.
[40] *Ibid.*, 329-30.
[41] Council of the European Union, "Strategic Compass" (2022), 26.
[42] "Ambiguous warfare" – sometimes linked to the notion of hybrid warfare – is associated with the attribution problem, i.e. the fact of not being able to determine the perpetrator of an attack (Hoorickx, "Countering 'Hybrid Threats'", 11).
[43] *Ibid*., 14.
[44] Joseph Henrotin, "La guerre hybride comme avertissement stratégique", *Stratégique*, 111, no. 1 (2016) : 20, https://www.cairn.info/revue-strategique-2016-1-page-11.htm. See also European Commission, *Joint Communication to the European Parliament and the Council: Joint Framework on Countering Hybrid Threats – A European Union Response*, JOIN/2016/018 final.

enabling them to create ambiguity concerning the nature and the origin of the attack[45]. Such ambiguity may make it harder to invoke the mutual assistance clause as the armed attack must be directed or launched against a targeted state from outside its territory for the clause to be activated[46].

Considering the complex reality of self-defence and the new ways of waging (hybrid) war, it is necessary to determine whether new threats can be qualified either as "armed attacks" in the legal sense of the term – in which case self-defence would be permitted, allowing Article 42(7) to be activated – or rather as modi operandi that do not allow a state to invoke self-defence, albeit they constitute unlawful acts under international law, such as interfering in internal affairs through massive disinformation campaigns. If we want to answer this question, we have to abide by the conditions for invoking Article 42(7), without losing sight of the national legal features of the Member States[47].

As explained above, and in accordance with the definitions of "self-defence" and "armed attack" generally accepted through the practice of states as well as by international jurisprudence and doctrine, a certain number of conditions must be met to trigger the mutual assistance clause. As a reminder, the state concerned must be the victim of an armed attack – whatever the weapons or techniques used – that has occurred, is ongoing or imminent, caused by a single act or a series of minor attacks, that is not only of significant scale and severity[48], but also directed or launched against the targeted state from outside its territory by a state or non-state actor. Furthermore, this violation must take place on the territory of the targeted state[49]. Three factors that must be taken into account in order for a new threat to be qualified as an armed attack and for the concerned state to be able to invoke Article 42(7) prove to be particularly difficult to identify: the geographical aspect, the severity of the attack and the attribution problem.

First, it is not easy to determine whether cyberspace[50], where cyberattacks take place and false information is spread, can be considered a territory in the geographical sense[51]. Indeed, it is often technically difficult to trace back the geographical, or even territorial, origin of a cyberattack. Furthermore, while false rumours find their breeding ground and diffusion field outside the territory

[45] Henrotin, "La guerre hybride comme avertissement stratégique", 11 and 14.

[46] On this topic, see the EU Council's Legal Service, "Article 42(7) TEU", 12 July 2016, document of the Council no. 11176/16, unpublished (limited) (available online in excerpts: https://data.consilium.europa.eu/doc/document/ST-11176-2016-INIT/en/pdf) as cited in André Dumoulin and Nicolas Gros-Verheyde, *La politique européenne de sécurité et de défense commune*, 326).

[47] See for example, Ministry of Armed Forces (France), "Droit international appliqué aux opérations dans le cyberspace", 2018; German Federal Government, "On the Application of International Law in Cyberspace", 2021.

[48] Zemanek, "Armed attack".

[49] An armed attack, for instance, should be distinguished from a "domestic terrorist threat". For more information on this topic, see the EU Council's Legal Service, "Article 42(7) TEU", as cited in Dumoulin and Gros-Verheyde, *La politique européenne de sécurité et de défense commune*, 326.

[50] Olivier Kempf defines cyberspace as "l'espace constitué de systèmes informatiques de toute sorte connectés en réseaux et permettant la communication technique et sociale d'informations par des utilisateurs individuels ou collectifs" [free translation: "the space made up of computer systems of all kinds connected in networks and enabling the technical and social communication of information by individual or collective users"] (Olivier Kempf, *Introduction à la cyberstratégie*, Paris, 2012, 14).

[51] On this topic, read: Frédérick Douzet, "La géopolitique pour comprendre le cyberspace", *Hérodote*, 152-153, no. 1-2 (2014), 3-21, https://www.cairn.info/revue-herodote-2014-1-page-3.htm; Alix Desforges, "Les représentations du cyberespace : un outil géopolitique", *Hérodote*, 152-153, no. 1-2 (2014): 67-81, https://www.cairn.info/revue-herodote-2014-1-page-67.htm.

of the targeted states[52], they may directly affect these countries and constitute "foreign interference in the information space" [53], especially on social media and other digital platforms[54].

Second, it is also challenging to ascertain whether the cyber or hybrid modi operandi can be regarded as an armed attack[55], be it a single incident or a series of minor malicious activities[56]. The decision of assigning this label depends on the scale of the attack as well as its impact on state actors, critical infrastructure or individuals. This approach is reflected in the national doctrines of most EU and NATO Member States. At the Brussels Summit in June 2021, NATO decided that both attacks in space and a serious cyberattack could lead to the invocation of Article 5[57]. Likewise, the (legal) doctrines of EU Member States are modelled on the Tallinn Manual, which focuses on the impact of cyberattacks as a decisive factor for them to be considered an armed attack by applying international law to cyberspace, and thus cyberwarfare[58]. France, for example, takes the view that a cyberattack causing significant human casualties or inflicting considerable physical or economic damage can be qualified as an armed attack provided that it has been directly or indirectly carried out by a state[59], such as an attack on critical infrastructure causing severe and large-scale damage. Scenarios in which digital piracy may lead to grounding a country's air force, keeping its naval force in the harbour or damaging nuclear centrifuges, as was the case in Iran in 2010, are worth considering[60]. The EU Council's Legal Service holds the view that the decision of qualifying a cyberattack as an "armed attack" must be taken on a case-by-case basis, based on the Tallinn Manual[61]. For example, the weaponisation of migration policies[62] – or in other words, the act of manipulating migration flows for destabilisation purposes – does not constitute an armed attack in the legal sense of the term, but rather falls under the umbrella of hostile, or even unlawful, acts that may lead to countermeasures (in addition to retaliatory measures, of course)[63].

[52] On this topic, read: Alexis Albarian, "Bref aperçu du traitement juridique de la désinformation en droit comparé : de la mise en place de sanctions strictement internes au recours à de véritables sanctions extraterritoriales", *Légicom*, 60, no. 1 (2018): 46, https://www.cairn.info/revue-legicom-2018-1-page-45.html.

[53] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* [COM(2020) 790 final], December 3, 2020: 22, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0790&from=FR.

[54] For more information on this topic, read: Estelle Hoorickx, "La lutte euro-atlantique contre la désinformation : état des lieux et défis à relever pour la Belgique", *Security & Strategy,* no. 150, October 2021, https://www.defence-institute.be/wp-content/uploads/2021/10/ss-150.pdf.

[55] The Legal Service of the Council of the EU states that the attack must reach a certain threshold of severity to be qualified as an armed attack and must therefore be distinguished from most of the terrorist attacks. EU Council's Legal Service, "Article 42(7) TEU", as cited in André Dumoulin and Nicolas Gros-Verheyde, *La politique européenne de sécurité et de défense commune*, 326.

[56] In this regard, see International Court of Justice, *Oil Platforms case* (Islamic Republic of Iran v. United States of America), judgment, 2003, para. 64.

[57] See NATO, "Brussels Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels", June 14, 2021: para. 32, https://www.nato.int/cps/en/natohq/news_185000.htm.

[58] Michael Schmitt (red), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

[59] Ministry of Armed Forces (France), "Droit international appliqué aux opérations dans le cyberspace", section 1.2.1.

[60] For more information on the possible (military) impact of cyberattacks, read Estelle Hoorickx, "L'implication de la Belgique dans la cyberstratégie euro-atlantique : état des lieux et défis à relever", *Security & Strategy* 139, February 2019, 11 and 13 (https://www.defence-institute.be/wp-content/uploads/2020/03/ss-139.pdf).

[61] EU Council's Legal Service, "Article 42(7) TEU", as cited in André Dumoulin and Nicolas Gros-Verheyde, *La politique européenne de sécurité et de défense commune*, 326.

[62] Elie Tenenbaum, "Migrants en Biélorussie : le casse-tête stratégique des 'menaces hybrides'", *Le Figaro*, November 12, 2021, https://www.lefigaro.fr/international/le-casse-tete-strategique-des-menaces-militaires-hybrides-20211112.

[63] Paddeau, "Countermeasures".

Finally, besides the breach of a rule of international law, the attack must be traceable back to the attacker for Article 42(7) to be invoked[64]. Practical evidence shows that, since 2001, states have primarily invoked self-defence after having been attacked by a non-state actor. In view of the national doctrines and the documents of the EU Council's Legal Service relating to Article 42(7) TEU[65], the clause is likely to be applicable to cyberspace as well – provided that the acts in question can be (in)directly traced back to a state entity. Indeed, while it can be technically difficult to prove that an individual is responsible for a cyberattack or a disinformation campaign, it is even more challenging to demonstrate that a state, which has every interest in withholding its identity for obvious geopolitical reasons, has ordered or tolerated such act. This attribution problem, which is a national sovereign prerogative, thus prevents any possible reaction – be it individual or collective – since it may be regarded as an act of aggression in the absence of sufficient evidence[66]. The decision of attributing a cyberattack to a specific actor is not only based on technical information, but also on the evaluation of the strategic context and the impact of the cyberattack beyond cyberspace (i.e. mainly physical, political or economic impact of an attack), taking into account the wider context, as emphasised by Germany's cyber doctrine[67].

Nonetheless, even when the attacker has been clearly identified, some countries remain reluctant to publicly accuse a state of aggression – even though this is a prerequisite for invoking collective self-defence. For example, a few years ago, when the *Bundestag* (German Parliament) and the Organisation for the Prohibition of Chemical Weapons (OPCW) suffered from cyberattacks by Russia and China, the EU preferred to impose sanctions on individuals (although they obviously acted, *de jure* or *de facto*, on behalf of a state) rather than on the two countries concerned, in order to avoid a political and legal escalation[68].

Conclusions and recommendations

Despite the shock caused by the Russian invasion of Ukraine, Member States do not place the same value on the mutual assistance clause of the Treaty on European Union (TEU): some favour their transatlantic bond with NATO while others – especially those EU countries that are not NATO members – believe that Article 42(7) is essential to guarantee their security against, in particular, the Russian threat. In any event, the mutual assistance clause of the Treaty on EU provides a useful, even vital, tool for building a European defence that is more sovereign and autonomous – a process that has only been accelerated by the war in Ukraine.

Nevertheless, invoking and triggering Article 42(7) TEU in case of a cyber or hybrid attack is not an easy task. A number of criteria related to the right of self-defence, which do not easily apply to new threats arising from hybrid warfare (also referred to as "ambiguous warfare"), must be met before the clause can be activated. Furthermore, Member States are currently still in need of a consistent and precise definition on new types of threats or attacks, despite the recently adopted

[64] This e-Note will not deal with the complex controversial argument that self-defence can also be invoked against non-state actors.

[65] EU Council's Legal Service, "Article 42(7) TEU", as cited in André Dumoulin and Nicolas Gros-Verheyde, *La politique européenne de sécurité et de défense commune*, 326.

[66] Wood, "International Law and the use of force: What happens in practice?", 350.

[67] German Federal Government, "On the Application of International Law in Cyberspace", 15.

[68] Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, July 30, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020R1125.

Strategic Compass. The lack of a common definition remains a gap that needs to be filled by the EU stakeholders in the near future. While it does not seem necessary to determine strict application criteria[69] for the mutual assistance clause, Member States should not only acquire a common understanding of new security phenomena – including cyber- and hybrid-related issues –, they should also record it in a political-strategic document so that Article 42(7) TEU can be activated quickly and efficiently, if need be. This requires an agreement on the criteria that need to be met for a cyberattack or hybrid campaign to be qualified as an armed attack, taking particular heed of its scale and severity. EU Member States could thus reach a political agreement, just as NATO did with its Article 5, on the possibility of triggering the mutual assistance clause when a large-scale cyberattack and/or attack in space is launched against one or several Member States. In any case, the Strategic Compass implies that mutual assistance could also be invoked against hybrid threats[70].

While Article 42(7) TEU provides a valuable legal basis for a collective response to an armed attack, it must be considered a measure of last resort. It should not serve as a legal basis to act or react against attacks that cannot be defined as an armed attack by their scope and impact. Indeed, in this case, diplomacy, retaliatory measures and countermeasures are to be preferred.

[69] Nicolas Gros-Verheyde, “À défaut d’article 5 de l’OTAN”.
[70] Council of the European Union, “Strategic Compass” (2022), 22.