Implementing Article 42.7 of the Treaty on European Union: Legal Foundations for Mutual Defence in the Face of Modern Threats

Boddens Hosang, J.F.R.; Ducheine, P.A.L.

DOI
10.2139/ssrn.3748392

Publication date
2020

Document Version
Final published version

UNIVERSITY OF AMSTERDAM

IMPLEMENTING ARTICLE 42.7 OF THE TREATY ON EUROPEAN UNION: LEGAL FOUNDATIONS FOR MUTUAL DEFENCE IN THE FACE OF MODERN THREATS

J.F.R. Boddens Hosang

P.A.L. Ducheine

Amsterdam Law School Legal Studies Research Paper No. 2020-71

Amsterdam Center for International Law No. 2020-35

Implementing Article 42.7 of the Treaty on European Union: Legal Foundations for Mutual Defence in the Face of Modern Threats

Dr. J.F.R. Boddens Hosang[1] and Prof. Dr. P.A.L. Ducheine[2]

42(7) Treaty on European Union: "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."

I. Introduction

Following the terrorist attacks in Paris in November 2015, the French government invoked Article 42, paragraph 7, of the Treaty on European Union (hereafter "Article 42.7") and created a precedent in terms of applying the Union's "mutual defence clause". As will be discussed briefly below, invoking this clause was legally complex, as it not only called into question the meaning and scope of the clause itself but also raised questions regarding the mechanisms for application and the obligations it imposed on the other Member States of the European Union (EU).[3] Moreover, the invocation sparked new interest in the clause itself and has renewed debate between the Member States and within the European Union's institutions as to its use, scope and (lack of) procedural aspects.

Although the mutual defence clause has its roots in a history more clearly related to traditional military threats, the current debates and the specific wording of the clause raise questions as to the possibilities of invoking the clause in the face of modern threats such as terrorism, cyber operations and hybrid warfare. While invoking the clause in response to the terrorist attacks in 2015 empirically establishes that the clause can be invoked in the face of terrorist attacks, and consequently against attacks by foreign non-state actors, the potential role of the clause in the face of less well-defined cyber or hybrid threats is subject to legal challenges and raises significant questions regarding the threshold requirement for invoking the clause.

Cyber-attacks of various kinds and in varying intensities occur on a continuous basis.[4] Although the possibility of cyber-attacks rising to the level of an armed attack has been argued convincingly,[5] and such attacks would then in any case warrant invoking the right of

---

[1] Dr. J.F.R. Boddens Hosang is senior external researcher with the University of Amsterdam's Center for International Law (ACIL) in the Law of Armed Conflict and Military Operations (LACMO) research program and external research fellow for Cyber Warfare at the Netherlands Defence Academy.

[2] Prof. Dr. P.A.L. Ducheine (Brigadier-General, Army Legal Service) is Professor in the Law of Military Cyber Operations at the University of Amsterdam and Professor in Cyber Warfare at the Netherlands Defence Academy.

[3] Traynor, I., "France invokes article 42.7, but what does it mean?" in *The Guardian*, 17 November 2015, available online at: https://www.theguardian.com/world/2015/nov/17/france-invokes-eu-article-427-what-does-it-mean.

[4] For an overview of recent major attacks, see the Center for Strategic & International Studies list at: https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents; or *Mitre Att&ck* at< https://attack.mitre.org/>, and Hackmageddon <https://www.hackmageddon.com/>. Several cyber security companies provide real-time world maps indicating ongoing malicious cyber activity, including FireEye (https://www.fireeye.com/cyber-map/threat-map.html), Check Point (https://threatmap.checkpoint.com/) and Kaspersky (https://cybermap.kaspersky.com/).

[5] See, for example, Schmitt, M.N. [ed.], *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, 2013, especially Rule 13 and associated commentary; AIV/CAVV - Advisory Council on International Affairs/Advisory Committee on Issues of Public International Law (2011) Cyber Warfare, Advisory Report no. 77/22, at:
www.aiv-advice.nl or <www.advisorycouncilinternationalaffairs.nl/documents/publications/2011/12/16/cyber-warfare>.

(collective) national self-defence under international law, questions remain as to the basis and modalities of multinational response and mutual support in response to cyber incidents below the threshold of an armed attack. For example, it may be questioned whether the specific wording of Article 42.7 and its reference to "armed aggression" would make the clause useful in that context or provide a basis for mutual support between the EU Member States.

The Russian annexation of the Crimean peninsula following a series of complex interventions in Ukrainian internal affairs has identified the need for an integrated approach to what is commonly referred to as "hybrid warfare".[6] Although not yet specifically defined, a common approach to hybrid threats identifies them as malicious activities threatening national security interest, without rising to the level of an actual (imminent) armed attack.[7] Nonetheless, the activities in question are in any case hostile and may, depending on the nature of the activities, fall under the concept of "aggression" as set forth, *inter alia*, in United Nations General Assembly resolution 3314 (XXIX). While the difference between "aggression" and "armed attack" is not always clearly definable, even less so when added to the concept of "the threat or use of force against the territorial integrity or political independence of any state" as set forth in Article 2, paragraph 4, of the Charter of the United Nations,[8] it can raise even further questions when compared to the term "armed aggression" in Article 42.7. The question, consequently, is whether Article 42.7 can provide a basis for mutual response by EU Member States in the face of hybrid threats not rising to the level of an armed attack.

In analysing these questions, this chapter will first (briefly) discuss the background, nature and scope of Article 42.7, including its relationship to Article 5 of the North Atlantic Treaty, Article 51 of the Charter of the United Nations and Article 222 of the Treaty on the Functioning of the European Union (TFEU).[9] Next, the issue of cyber threats and mutual

---

[6] Ducheine, P.A.L., "Nationale veiligheid en hybride dreiging: twee kanten van dezelfde medaille," in *Magazine nationale veiligheid en crisisbeheersing*, 2016 - 5/6.

[7] See National Coordinator for Security and Counterterrorism (2019) *Çhimaera - An analysis of the 'hybrid threat' phenomenon*, The Hague, p. 9: "In essence the term refers to threats that can assume various forms and impact on multiple national security interests and thus be categorised as a 'threat to national security'. The word 'hybrid' refers to the use of a mix of tactics and to the threat's asymmetrical nature, polymorphous manifestation and wide-ranging impact (on multiple national security interests). Instead of referring to a 'hybrid threat', it is better to speak of a threat to national security." At <https://english.nctv.nl/themes/state-threats/documents/publications/2019/09/05/analysis-of-the-%E2%80%98hybrid-threat%E2%80%99-phenomenon>.

[8] See also Boddens Hosang, J.F.R., *Rules of Engagement and the International Law of Military Operations*, Oxford, 2020, pp. 53 – 54.

[9] Article 222 Treaty on the Functioning of the European Union

1. The 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:

(a) - prevent the terrorist threat in the territory of the Member States;
- protect democratic institutions and the civilian population from any terrorist attack;
- assist a Member State in its territory, at the request of its political authorities, in the event of a terrorist attack;

(b) assist a Member State in its territory, at the request of its political authorities, in the event of a natural or man-made disaster.

2. Should a Member State be the object of a terrorist attack or the victim of a natural or man-made disaster, the other Member States shall assist it at the request of its political authorities. To that end, the Member States shall coordinate between themselves in the Council.

3. The arrangements for the implementation by the Union of the solidarity clause shall be defined by a decision adopted by the Council acting on a joint proposal by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy. The Council shall act in accordance with Article 31(1) of the Treaty on European Union where this decision has defence implications. The European Parliament shall be informed.

European defence will be discussed, followed by a discussion of hybrid threats and mutual European defence. Finally, a few concluding remarks will be presented.

II. Background and Purpose of Article 42.7

As Article 42.7 is also discussed elsewhere, the following discussion of the clause will be brief and will focus primarily on the aspects and elements relevant for the subsequent discussions of mutual European defence against cyber and hybrid threats.

A. Genesis and Scope of Article 42.7

The concept of mutual defence between European nations outside the context of the North Atlantic alliances dates back, of course, to the early 1950s and the so-called "Pleven plan" for the European Defence Community (EDC).[10] Although the EDC did not materialise in the form intended, the Western European Union (WEU) which arose in 1954 on the basis of the modified Brussels Treaty did create the basis for mutual defence between European States outside the context of the 1949 North Atlantic Treaty. Leaving aside the initially dormant, but later active role of the WEU,[11] the principal element of interest for the present discussion is the wording of Article V relating to the mutual defence clause of the WEU. Contrary to the discretionary wording of the *casus foederis* in Article 5 of the North Atlantic Treaty,[12] as will be discussed below, the mutual defence obligations between the WEU Member States was clearly obligatory and left little margin for national consideration. Put simply, the clause set forth an obligation for the WEU Member States to assist any WEU Member State following an armed attack on that State, and required such assistance to encompass "all the military and other aid and assistance in their power."

Following the introduction of the concept of a Common Foreign and Security Policy (CFSP) in the Maastricht Treaty in 1993 and the subsequent development of that concept in combination with the later concept of a Common Security and Defence Policy (CSDP) in the

---

For the purposes of this paragraph and without prejudice to Article 240, the Council shall be assisted by the Political and Security Committee with the support of the structures developed in the context of the common security and defence policy and by the Committee referred to in Article 71; the two committees shall, if necessary, submit joint opinions.

4. The European Council shall regularly assess the threats facing the Union in order to enable the Union and its Member States to take effective action.

[10] For a more extensive discussion of the history of Article 42, see, *inter alia*, Fischer, M.G and Thym, D., "Article 42 [CSDP: Goals and Objectives, Mutual Defence]" in Blanke, H.J. and Mangiameli, S. [eds.], *The Treaty on European Union: A Commentary*, Springer, 2013.

[11] Although the WEU was never "activated" for the role of mutual defence, the organisation did carry out a number of peace operations, including the so-called Petersberg tasks, including the minesweeping operations in the Persian Gulf (1987 – 1988), coordinating European States' contributions to operations Desert Shield and Desert Storm (1990 – 1991), the maritime embargo off the coast of the former Yugoslavia (Sharp Guard, 1993), the Multinational Advisory Police Element (MAPE) in Albania (1997 – 2001) and the WEU Demining Assistance Mission (WEUDAM) in Croatia (1999 – 2001).

[12] "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 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."

Treaty of Nice (2003) and Treaty of Lisbon (2007 – 2009), the relationship between the EU and the WEU changed from complementary institutions to integrating the WEU into the EU. But while all the (full) Member States of the WEU were also members of the North Atlantic Treaty Organisation (NATO), the same is, of course, not the case for the EU. Moreover, the relationship between NATO and the EU required redefinition as regards the policies and commitments of the NATO Member States within the EU, now that mutual defence was being incorporated into the EU and embedded in the Treaty on European Union (TEU).[13]

Focusing specifically on the mutual defence clause, however, it is clear from the wording of Article 42.7 that the original WEU version has undergone some changes. Although the obligatory nature is still present in the wording, the "trigger" criterion has been changed from "armed attack" to "armed aggression". Furthermore, the specific reference to military assistance has been discarded and instead the Member States must provide assistance by "all the means in their power." Although that clearly includes the option of military assistance, the lack of a specific reference thereto may be explained by the introduction of a new element: the additional sentence emphasizing that the clause "shall not prejudice the specific character of the security and defence policy of certain Member States," clearly referring to the position of the traditionally neutral States such as Ireland.

Examining firstly the "trigger" element, it may be questioned whether the term "armed aggression" differs substantially or normatively from the previous WEU wording of "armed attack." While it may be argued that "armed aggression" provides a wider scope and could include other (armed) activities than the concept of "armed attack" as set forth in Article 51 of the UN Charter,[14] it should be noted that the phrasing may simply be an EU translation of the original French text referring to "*aggression armée*" as also used in the French version of Article 51 of the Charter of the United Nations.[15] This more limited interpretation, including only the "classic" approach to collective self-defence rather than expanding the opportunities for resorting to the use of military force, would, in turn, be an appropriate acknowledgment of the fact that, notwithstanding the existence of Article 42.7, the EU is not comparable to NATO in terms of the purpose or scope of the organisation as a whole.

The wording of the "trigger" element in Article 42.7 does, however, raise questions as regards its interaction with what is commonly referred to as "the solidarity clause" set forth in Article 222 TFEU.[16] If "armed aggression" is intended to broaden the scope, or perhaps lower the threshold for invocation, of Article 42.7, and if, as will be discussed briefly below, attacks by non-state actors can trigger mutual defence, it may be questioned whether large-scale attacks by foreign terrorist fighters should be considered a trigger for Article 42.7 TEU or Article 222 TFEU. This question gained relevancy as a result of the invocation of Article 42.7 following the 2015 terrorist attacks in Paris mentioned in the introduction.

Given the nature and scope of the solidarity clause and given the original intentions behind Article 42.7, it may be argued that the choice between the clauses in response to a terrorist attack is one of scope. This would mean that terrorist attacks which do not meet the criteria for invoking national self-defence as that concept is understood under international law

[13] See especially the second paragraph of Article 42, paragraph 2, of the TEU.
[14] See, for example, Fischer & Thym, *op. cit.* note 10, p. 1224.
[15] Ibid. See also Boddens Hosang, *op. cit.* note 8, footnote 11 on p. 54. The view that the phrasing is simply a literal translation of the French is also supported by Sari; see Sari, A., "The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats," in *Harvard National Security Journal*, Vol. 10, 2019, p. 418.
[16] See *supra* note 9.

would warrant invoking the solidarity clause, while terrorist attacks which do meet those criteria would offer a choice between invoking the solidarity clause of Article 222 TFEU or Article 42.7. Clearly France chose the latter in 2015.

As regards choosing between the two clauses in these specific cases, note that there is a significant difference as regards the subsequent decision making and implementation. While the role of the EU institutions is extensive and specific in regards to the solidarity clause,[17] no such procedural or institutional framework exists for Article 42.7, leaving its implementation up to the Member States.[18] Finally, as has been noted by a several authors,[19] invoking the solidarity clause of Article 222 TFEU means that the State in question admits to being "overwhelmed"[20] by the situation and that it is no longer capable of resolving it through its own national instruments and capabilities, which may be politically unpalatable. Although that does not, of course, change the legal parameters for invoking Article 42.7, the apparent political preference for (or rather the more politically acceptable nature of) Article 42.7 does provide a basis for exploring the ways and situations in which that provision may be invoked.

B. Relationship with Article 51 of the Charter of the United Nations

Several aspects of the relationship between Article 42.7 TEU and Article 51 of the Charter of the United Nations (UNCH) have already been discussed above. Nonetheless, a few general observations regarding that relationship and, more specifically, regarding national self-defence may be considered relevant to this discussion.

Given the genesis of Article 42.7 and its intrinsic purpose, it is clear that the clause in any case encompasses the right to collective national self-defence, as also clearly indicated by the cross-reference to Article 51 UNCH contained in the clause itself. The right of national (individual and collective) self-defence as set forth in Article 51 UNCH is, as also literally stated in that provision, an inherent right[21] but nonetheless governed, in the modern system of international law regarding peace and security, by the provisions of Article 51 UNCH.[22] That means, *inter alia*, that the invocation of the right of national self-defence is predicated on a prior armed attack against the State invoking its right of self-defence. Although, as was discussed above, the French version of the UNCH refers in this context to "aggression armée" instead of the phrase "attaque armée" as used in the French version of Article 5 of the North Atlantic Treaty, it is questionable whether any normative effect should be attributed to that choice of wording.

---

[17] See Council Decision 2014/415/EU of 24 June, 2014.

[18] See extensively Nováky, N.I.M., "The Invocation of the European Union's Mutual Assistance Clause: A Call for Enforced Solidarity," in *European Foreign Affairs Review*, Vol. 22, no. 3, 2017, also presenting an analysis of French motives for invoking Article 42.7 instead of Article 222 TFEU or Article 5 NATO.

[19] Sari, *op. cit.* note 15, p. 424; Nováky, *op. cit.* note 18, p. 367, Bakker, A. [et al.], *Spearheading European Defence: Employing the Lisbon Treaty for a Stronger CSDP*, Clingendael Report, 2016, p. 24.

[20] Although Article 222 TFEU itself does not set forth such a threshold, the Council Decision implementing the solidarity clause (*op. cit.* note 14) specifies in Article 4, paragraph 1, that a Member State may invoke the clause "if, after having exploited the possibilities offered by existing means and tools at national and Union level, it considers that the crisis clearly overwhelms the response capabilities available to it."

[21] As also stated by the International Court of Justice (ICJ); see *inter alia*, ICJ, *The Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)*, 8 July 1996, paragraph 96.

[22] Gill, T.D., "Legal Basis of the Right of Self-Defence Under the UN Charter and Under Customary International Law," in Gill, T.D. and Fleck, D. [eds.], *The Handbook of the International Law of Military Operations*, 2nd Ed., Oxford, 2015, esp. pp. 214 – 216; Dinstein, Y., *War, Aggression and Self-Defence*, 5th Ed., Cambridge, 2011, esp. pp. 191 – 193.

It is without question that the notions of national self-defence and armed attack also include a right to defend against an imminent attack, commonly referred to as anticipatory self-defence,[23] and that the common view in international law following the attacks on the United States on 11 September, 2001, acknowledges that, under certain conditions, attacks by non-state actors may also trigger the right of national (collective) self-defence.[24] In other words, there is no legal barrier against invoking national self-defence, including collective self-defence on the basis of Article 42.7 and similar provisions, against an (imminent) attack by, for example, foreign terrorist fighters, provided the various criteria are met.[25] It should be noted, especially in connection with the tactics applied by some non-state actors and as further discussed below, that the trigger for (collective) national self-defence may also be met on the basis of several smaller incidents involving the use of force, provided those incidents are related to each other, have a common goal and are part of a common strategy (see section III below).[26]

Finally, it may be the questioned whether the reference to Article 51 UNCH in the wording of Article 42.7 encompasses both the "trigger" element of Article 42.7 and the subsequent obligation of rendering assistance, thus limiting the scope of Article 42.7 to the situations covered by Article 51 UNCH, or whether the reference "merely" indicates that any assistance rendered must comply ultimately with Article 51 UNCH. Here, too, the wording of Article 42.7, the genesis of that provision, and the placement of the reference to Article 51 UNCH in the provision all seem to indicate the former. Consequently, the relationship between Article 42.7 TEU and Article 51 UNCH appears to be identical to the relationship between Article 5 NATO and Article 51 UNCH, meaning that both the TEU and the NATO provisions are expressions of (modalities for) collective defence against an (imminent) armed attack as set forth in Article 51 UNCH.

C. Comparison with Article 5 of the North Atlantic Treaty

Although Article 42.7 refers specifically to the "commitments" of the EU Member States who are also members of NATO, and the role of NATO as "the foundation of their collective defence" for those States, there is of course no automatic link between Article 42.7 TEU and Article 5 NATO in the sense that one triggers the other. The decision to invoke the provisions in question remains up to the Member States of the respective organisations. It is interesting to note, however, that although the two provisions have similar (or perhaps identical) purposes, a few significant differences exist between the two provisions.

---

[23] See, for an extensive discussion of the right of anticipatory self-defence, Tibori Szabó, K., *Anticipatory Action in Self-Defence: Essence and Limits under International Law*, Springer, 2011. Note that anticipatory self-defence should not be confused with pre-emptive self-defence. While the former is legal in the face of an imminent attack and subject to specific criteria, the latter, focusing on removing a potential threat before it can possibly develop to the level of an (imminent) attack, constitutes a violation of international law.

[24] See also, *inter multos alia*, Gill, T.D., "The 11th of September and the International Law of Military Operations," inaugural lecture delivered on the appointment to the chair in Military Law at the University of Amsterdam, 20 September 2002; Trapp, K.N., "Can Non-State Actors Mount an Armed Attack?" in Weller, M. [ed.], *Oxford Handbook of the Use of Force in International Law*, Oxford, 2015; Dinstein, *op. cit.* note 22, pp. 227 – 230.

[25] Although a full discussion of those criteria falls outside the scope of this chapter, regard should be had to the scale of the attack and its consequences, the fact that the attacking party must be foreign (there is no right of self-defence against a State's own population under international law; such situations are governed by national law), and the level of organization of the attack (i.e. not consisting of separate and unrelated incidents carried out by separate and unrelated actors).

[26] Gill, T.D. and Ducheine, P.A.L., "Anticipatory Self-Defence in Cyber Warfare", in Schmitt M. [ed.], *Cyber War and International Law*, 89 International Law Studies 2012, pp. 438-471, p. 443, via <https://digital-commons.usnwc.edu/ils/vol89/iss1/6/>.

In terms of the obligations of the Member States following invocation of the provision in question, the NATO version appears to leave room for national discretion, while the EU version appears more obligatory. While both require a response from the other Member States to assist the attacked Member State, the NATO version leaves the nature of that response subject to what each Member State considers necessary. The EU version, on the other hand, requires a response "by all the means in their power." Given, however, the lack of any institutional or structured procedures in both organizations for the application of the provisions in question, it is doubtful whether this difference will *de facto* result in real differences between the organizations, as implementation will in both cases require bilateral consultations between the stricken State and the assisting State.[27]

While Article 42.7 TEU appears more obligatory in its effect than Article 5 NATO, a converse situation applies as regards the scope of the provisions. Article 5 NATO applies to all the Member States of NATO without exception, meaning its invocation provides equal obligations for all. Article 42.7 TEU, on the other hand, specifically addresses "the specific character of the security and defence policy of certain Member States," referring to the neutral policy of a number of EU Member States. As has been pointed out in academic literature, this means that following an invocation of Article 42.7, the EU Member States adhering to such a policy of neutrality must determine which position they wish to take in the context of the circumstances ruling at that time and which aid or assistance they can provide without compromising their national policies.[28]

III. Cyber Threats and Mutual European Defence

The concept of cyberspace, a term introduced by William Gibson,[29] can be understood as "to cover all entities that are or may potentially be connected digitally".[30] Cyberspace, manmade territory, is a vital part in the so-called information environment which in turn comprises three dimensions: cognitive, virtual and physical. This environment is sub-divided in seven layers consisting of: social groups, psyche, cyber-identities, cyber-objects, hardware, ordinary tangible objects and geographical locations (of all entities).[31] Cyberspace itself comprises two layers in the virtual dimension - cyber-identities (e.g. email accounts) and cyber-objects (software (including firmware, applications) protocols and data) – and one physical layer – hardware (e.g. computers, routers, cables, servers).[32]

---

[27] See also Nováky*, op. cit.* note 18, esp. pp. 370 – 371.
[28] Fischer & Thym, *op. cit.* note 10, pp. 1228 – 1230.
[29] Gibson, W., *Neuromancer*, Penguin Press, 2018.
[30] Netherlands' Defence Cyber Strategy, 2012, (UK version): "Cyberspace is understood to cover all entities that are or may potentially be connected digitally. The domain includes permanent connections as well as temporary or local connections, and in all cases relates in some way to the data (source code, information, etc.) present in this domain". Original (in Dutch): *Parliamentary Papers II* 2011-2012, 33 321, no. 1.
[31] See Ducheine, P. and van Haaster, J., "Fighting Power, Targeting and Cyber Operations", in Brangetti, P., Maybaum, M. and Stinissen, J [eds.] *Proceedings of the 6th International Conference on Cyber Conflict*, 2014, Tallinn: CCDCOE, pp. 303-328; Ducheine, P., van Haaster, J., van Harskamp,R., "Manoeuvring and Generating Effects in the Information Environment", in Ducheine, P. and Osinga F. [eds.], *Winning without killing – The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*, NLARMS Netherlands Annual review of Military Studies 2017, TMC Asser Press, The Hague 2017, pp. 155-180, online via SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2979287>.
[32] van Haaster, J., *On Cyber – The utility of military cyber operations during armed conflict* (PhD University Of Amsterdam), 2019, p. 136, via < https://pure.uva.nl/ws/files/37093787/Thesis.pdf>. Until artificial intelligence takes over, cyberspace is created and used by people. People themselves take part in the physical dimension (body, acts) and are part of the cognitive dimension (either as individuals with psyche, decision making or as a group or culture).

Cyberspace, accessible to some 4.1 billion people worldwide,[33] is used for a range of benevolent and legitimate as well as malevolent activities by both States and non-state actors. Most activities have a benign character related to commercial and private uses of the internet and social media.[34] However, cyberspace is also used for malignant purposes: espionage, theft, crime in general, subversion, social engineering and even warfare.[35] Combined with technical and human failure, these activities pose a threat to cyber security.[36] Some, if not most of these threats are easily characterised as cyber attacks.[37]

Nevertheless, only a small portion of these threats may be characterised as an attack in the meaning of the *jus ad bellum*. To date, arguably, only one or two of these attacks actually qualified as an armed attack in the meaning of the UN Charter. These, and the ones that are foreseeable in theory, will be covered first (section III A). Most of the threats, however, fall short of this qualification, but may nevertheless be relevant in other terms as will be addressed in section III B.

A. Cyber Attacks as Armed Attack

Departing from the position that "armed aggression" in Article 42.7 EU Treaty reads as "armed attack" in the meaning of the UN Charter, in order to answer the question whether, and what kind of, cyber attacks qualify as armed attacks, the classic interpretation of 'armed attack' should be clear in the first place (see section Classic Armed Attack, below). Secondly, this classic interpretation of an armed attack, complicated as it is, should be updated in view of recent events that have had an impact on the interpretation of the *jus ad bellum*: the terrorist attacks of 9/11 (2001) and the terrorist attacks in France (2015) (see section The Impact of 9/11 and Bataclan, below). Thirdly, the likelihood and modalities of a cyber armed attack will have to be addressed (see section Cyber Armed Attack, below). And finally, the issue of the reading of 42.7 deserves attention (see section Armed Attack/Armed Aggression, below).

(1) Classic Armed Attack

Based on the textual interpretation of Article 51 UN Charter, analysis of customary law and supplementary sources (such as international case law), an armed attack has been defined as "a use of force which originates from outside the target State's territory, rising above the level of a small scale isolated armed incident or criminal activity, which is directed against a State's territory, its military vessels or aircraft in international sea or airspace or lawfully present on another State's territory, or in certain situations directed against its nationals located abroad."[38] Summarizing the requirements briefly, first of all, an armed attack involves the use of force, normally understood to be military force. In addition, it requires a significant use of force,

[33] International Telecommunication Union, *Measuring digital development - Facts and figures 2019*, p. 1, via <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf>.
[34] Ducheine, P.A.L. and Pijpers, B.M.J., "The Notion of Cyber Operations", in: Tsagourias, N., and Buchan, R., [eds.], *The Research Handbook on the International Law and Cyberspace*, 2nd edition, Cheltenham: Edward Elgar (forthcoming), online at < https://ssrn.com/abstract=3575755>.
[35] National Cyber Security Centre (NCSC), *National Cyber Security Assessment 2019*, via <https://english.ncsc.nl/binaries/ncsc-en/documents/publications/2019/09/13/cyber-secrurity-assessment-netherlands-2019/Cyber-+Security-+Assessment-+Netherlands-+2019.pdf>.
[36] "Cyber security refers to efforts to prevent damage caused by disruptions to, breakdowns in or misuse of ICT and to repair damage if and when it has occurred.", in: National Cyber Security Centre, *Netherlands' National Cyber Security Strategy - 2 From awareness to capability*, 2013, via <https://ccdcoe.org/library/strategy-and-governance>.
[37] Ducheine and Pijpers, *op. cit*. note 34.
[38] Gill and Ducheine, *op. cit.* note 26, p. 443; and Gill, *op. cit.* note 22, p. 213, Rule 8.01.

usually measured in terms of "scale and effects".[39] Third is the transnational or cross-border aspect of an armed attack. Normally, armed attacks are conducted by the armed forces of a State, launching or conducting a military operation against targets in or belonging to another State.

(2) The Impact of 9/11 and Bataclan

As demonstrated above (Section II), the notion of armed attack under the *jus ad bellum* has been impacted in three distinct ways by the 9/11 terrorist attacks against the United States of America and the subsequent response. Additionally, the 2015 terrorist (Bataclan *et al*.) attacks, and the ensuing French and European Union's reaction, are of relevance too.

First of all, it became clear from State practice and statements, that a non-state actor could qualify as the author of an armed attack. Secondly, it was obvious that an armed attack (now) could be 'produced'/generated by non-military means and alternative methods. Thirdly, as could be derived from the statements by States responding to the armed attack,[40] an armed attack could also comprise a series of smaller attacks, produced by a common author against the same target State, when these attacks are reasonably connected in geographic and temporal terms.[41] These three facets/aspects of armed attack will be used in relation to cyberspace.

Firstly, cyberspace is the realm where states no longer have the prerogative of affecting other State and non-state actors.[42] The information, techniques, capacities and capabilities offered in cyberspace are almost equally available to individuals, groups, companies and (quasi) States.[43] Unlike weaponry and military equipment, the proliferation of skills, knowledge, software and hardware can hardly be stopped.[44] Apart from the fact that cyber operations are commonly conducted by States through their State organs, such as intelligence services or military units,[45] cyberspace also houses less clear affiliations between States and recognizable groups of cyber operators ('hackers') such as Cozy Bear, Fancy Bear or the

[39] ICJ, *Case Concerning Military and Paramilitary Activities In and Against Nicaragua* (Nicaragua vs. United States), Merits, 27 June 1986, paragraph 195**.** Also: Gill, *op. cit.* note 22, p. 216, Rule 8.03: "a reasonably significant use of force".

[40] See i.a. UN Doc. S/2001/947 (Letter dated 7 October 2001 from the Chargé d' affaires a.i. of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the United Nations Addressed to the President of the Security Council), p. 1.

[41] Gill and Ducheine, *op. cit.* note 26,

[42] Of note is that among States differences of opinion exist as to whether self-defence can be used against a non-state group. France takes the position that – in general – it cannot apply self-defence against the a non-state author, whose acts are not attributable to a State. The nuance being that France based its intervention against Da'esh in Syria firstly on the principle of collective self-defence in favour of Iraq, then, after the Bataclan attacks of 13 November 2015, on the basis of individual self-defence. See: France, *International law applied to operations in cyberspace*, 2019, p. 9, via: <https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf>.

[43] Dunn Cavelty, M., and Wenger, A., "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science", in: *Contemporary Security Policy - Special issue: Cyber Security Politics* 41, no. 1 (January 2, 2020): 5 – 32. Online <http://www.tandfonline.com/doi/abs/10.1080/13523260.2019.1678855>.

[44] See for instance the Wassenaar Arrangement: Ruohonen, J. and Kimppa. K.K., "Updating the Wassenaar Debate Once Again: Surveillance, Intrusion Software, and Ambiguity". In: *Journal of Information Technology & Politics* 16, no. 2 (April 3, 2019): 169–186, online <http://www.tandfonline.com/doi/abs/10.1080/19331681.2019.1616646>.

[45] See Sanger, D., *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power,* Crown, 2012, p. 188 ff; and Sanger, D., *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, Scribe, 2018, Chapter 1 - The Original Sins, describing that the US National Security Agency and Israel's Unit 8200 are (with partners) responsible for Operation Olympic Games, i.e. the use of Stuxnet against Iranian nuclear facilities.

Lazarus Group.[46] Arguably, some of these groups have affiliations with State organs.[47] APT 28, also known as Fancy Bear, for instance, has been attributed to Russia's Main Intelligence Directorate of the Russian General Staff (the GRU) by a U.S. Department of Justice indictment.[48] This group ostensibly compromised the Democratic campaign in 2016 in an attempt to interfere with the U.S. presidential election. The Sandworm Team, likely a group of pro-Russian hacktivists with less clear links, has been connected with the disruption of Ukrainian energy services in December 2015, cutting off power to some 200.000 household for hours.[49]

Noting the dependencies of economies, societies, households and even individuals on cyberspace, it is noteworthy that apart from States, non-state actors have proven they possess capabilities of threating and affecting vital interests.[50] As such, and apart from the few known cases, launching cyber operations that potentially equal the effects of an armed attack, as was the case on 9/11, either by State or non-state actors, in not just a theoretical chance or risk.

The second factor of relevance in this respect is the fact that most, if not all, of the capacities required to launch harmful operations are not designated as military means. Whether employed by the military, other state organs, or by non-state actors with or without involvement of states, the capacities used – software, cyber-identities, hardware – could be 'civilian' in nature. Contrary to classis military instruments ('weapons') and methods ('warfare'), cyber instruments do not automatically fit into the conventional instruments-based approach, but rather in an effect-based approach related to the notion of armed attack.[51] As the 9/11 attacks also demonstrated, these unorthodox methods of generating force, using ordinary means, can also generate the same effects as classic military force could have done. It is noteworthy that two Chinese military researchers, as early as 1999, foresaw that "one hacker + one modem causes an enemy damage and losses almost equal to those of a war".[52] This doctrinal and

---

[46] For an overview of these groups, commonly referred to as Advanced Persistent Threats (or APTs), see the list produced by Mitre-Att&ck, at <https://attack.mitre.org/groups/>.

[47] See Mitre Att&ck, via <https://attack.mitre.org/groups/G0007/>. Also e.g. Booz Allen, *Bearing Witness: Uncovering the Logic Behind Russian Military Cyber Operations*, 2020, at <https://www.boozallen.com/c/insight/publication/the-logic-behind-russian-military-cyber-operations.html>.

[48] See US Department of Justice, *USA v. Viktor Borisovich Nethyksho et al*, Case 1:18-cr-00215-ABJ, Filed 13 July 2018, at <https://www.justice.gov/file/1080281/download>.

[49] Hultquist, J., *Sandworm Team and the Ukrainian Power Authority Attacks*, (2016, January 7), at: Fire-eye, via <https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html>, and Michael Assante, M., *Confirmation of a Coordinated Attack on the Ukrainian Power Grid*, (2016, January 6), at: SANS, via < https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/>.

[50] E.g. Netherlands Scientific Council for Government Policy (WRR), *Preparing for Digital Disruption (Summary)*, WRR-report no. 101 (Summary). Den Haag, WRR(2019), via <https://english.wrr.nl/topics/digital-disruption/documents/reports/2019/09/24/preparing-for-digital-disruption>;
Algemene Rekenkamer, *Strengthening the digital defences: the cyber security and critical water structures*, Den Haag, ARK, 2019. via <https://english.rekenkamer.nl/publications/reports/2019/03/28/strengthening-the-digital-defences-the-cyber-security-of-critical-water-structure>;
Dutch Safety Board, *Patient safety during IT outages in hospitals*, The Hague, Onderzoeksraad voor de Veiligheid, 2020, via <https://www.onderzoeksraad.nl/en/media/attachment/2020/2/13/patient_safety_during_it_outages_in_hospitals.pdf>.

[51] For a critique on the effect-based approach (as applied in the Tallinn Manual 2.0), see Boer, L.J.M., "Restating the Law "As It Is": On the Tallinn Manual and the Use of Force in Cyberspace". In: *Amsterdam Law Forum*, 2013. 5(3), 4-18; and Boer, L.J.M. , "Echoes of Times Past: On the Paradoxical Nature of Article 2(4)", *Journal of Conflict & Security Law* (2014), 1.

[52] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999, p. 199, via <https://archive.org/details/Unrestricted_Warfare_Qiao_Liang_and_Wang_Xiangsui/mode/2up>.

strategic observation, however, is in line with the International Court of Justice's Nuclear Weapons Advisory Opinion.[53] According to the Court, the "provisions [Chapter VII, i.a. Article 51 UN Charter] do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed."[54] The approach is also consistent with the *opinio iuris* expressed by States,[55] by State practise,[56] and with the findings in legal doctrine, including the international group of experts (IGE) that contributed to the Tallinn Manuals.[57]

The third factor involves the fact that, according to some views, armed attack can consist of "a series of smaller scale uses of force which are conducted by the same author against the same target State which are reasonably connected in geographical and temporal terms and constitute what is in effect a phased armed attack."[58] This view is often referred to as the 'accumulation of events' theory, also referred to as 'pin-prick' armed attack or the 'Nadelstichtaktik'.[59] Pursuant to this theory, a series of smaller attacks, that on their own merits do not meet the criteria for an armed attack, could, when viewed in combination, jointly be seen as having met those criteria.

This would require that the series of attacks can, firstly, be attributed at all, and, secondly, be attributed to a common author. Hence, it involves (i) the capability of detecting an attack, (ii) the capability of technical or 'forensic' attribution of the attacks, and (iii) the capability of legal attribution of the attacks to a common author (operating from abroad).[60] Thirdly, the series of attacks should be directed against targets in or belonging to a single State. Fourthly, the series of attacks are – somehow – related in terms of time and location. And

---

[53] See *supra* note 21.

[54] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1. C.J. Reports 1996, p. 226, § 39.

[55] See i.a. the overview in Roguski, P., *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*. Policy Brief: The Hague Forum for Cyber Norms, 2020, p. 9, via <https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views>, referring to the *jus ad bellum* and other International Law statements made by Australia, Germany, France, the Netherlands, the United Kingdom and the United States.

[56] See the US' and UK's response in self-defence after 9/11 (i.a. UN Doc. S/2001/947 (Letter dated 7 October 2001 from the Chargé d' affaires a.i. of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the United Nations Addressed to the President of the Security Council), p. 1;
the UN Security Council Resolution implying that the 9/11 attacks had triggered the right to self-defence (UN Doc. S/RES/1368 (2001) (SC Resolution 1368 Threats to international peace and security caused by terrorist acts) and UN Doc. S/RES/1373 (2001) (SC Resolution 1373 Threats to international peace and security caused by terrorist acts);
and see NATO's confirmation – and subsequent contributions to Operation Enduring Freedom, that it regarded the terrorist assault as an armed attack, see NATO (2001), Oct 8 Press Release (2001) 138: Statement by NATO Secretary General, Lord Robertson, 8 October 2001, via <http://www.nato.int/docu/pr/2001/p01-138e.htm>; and NATO (2001), Sep 12 Press Release (2001) 124: Statement by the North Atlantic Council, 12 September 2001, via <http://www.nato.int/docu/pr/2001/p01-124e.htm>.

[57] Schmitt M.N., et al [ed], *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: CUP, 2017, Rule 71, § 5, p. 340-341: "the critical factor was whether the effects of a cyber operation, as distinct from the means used to achieve the effects, were analogous to those that would result from an action otherwise qualifying as an kinetic armed attack."

[58] Gill and Ducheine, *op. cit.* note 26, p. 445.

[59] See inter alia: Blum, Y.Z. "State Response to Acts of Terrorism", in: 19 German Yearbook of International Law, (1976), 223-237;
and Ducheine P.A.L. and Pouw, E.H., "Operation Change of Direction: A Short Survey of the Legal Basis and the Applicable Legal Regimes", in: de Weger, M.J. and Osinga, F.P.B et al [eds*.], Netherlands Annual Review of Military Studies - Complex operations: Studies on Lebanon (2006) and Afghanistan (2006-present*), 2009, pp. 51-96, esp. pp. 61-63, with accompanying notes.

[60] Bijleveld, A., "We have to steer the cyber domain, before it steers us" (keynote speech), in: *Militair Rechtelijk Tijdschrift* 2018, via <https://puc.overheid.nl/mrt/doc/PUC_248478_11/1/>.

fifthly, the series of attacks, or the attack as whole, constitutes force of sufficient gravity in terms of scale and effects as to qualify as an armed attack.

(3) Cyber Armed Attack

Pursuant to the analysis set out above, it is be to expected that some cyber operations indeed qualify as armed attacks. Most likely, it is rather obvious that some military cyber operations indeed would so qualify. Military cyber operations refer to "the employment of cyber capabilities with the primary purpose of achieving military goals in or by the use of cyberspace."[61] Military cyber operations implying the use of force across international borders, with scale and effects comparable to regular armed attacks, could be viewed as armed attacks.[62] The notion of 'scale and effect' captures both qualitative and quantitative factors.[63] These cyber operations constituting force (and attack) should be analogous with (the scale and effects of) kinetic and non-kinetic operations that would be described as force and, subsequently, armed attack.[64]

However, as demonstrated above, it could also be the case that other State organs and non-state actors whether or not affiliated with a State, are the author of a cyber operation/attack.[65] When applying the accumulation of events theory, the actor responsible should be a single actor, State or non-state.

Looking at the scale and effects requirement, it is evident that cyber operations of a comparable scale and effects in relation to classic military armed attacks could, in theory, qualify as such.[66] This is in line with the interpretation of a number of States. Distinction should be made however, between cyber operations with physical effects on the one hand, and non-physical effects on the other hand.

The IGE contributing to the Tallinn Manuals agreed on the fact that a cyber operation that "seriously injures or kills a number of persons or that causes significant damage to, or

[61] Ducheine, P.A.L., "Military Cyber Operations", in: Gill & Fleck, op. cit. note 22, Chapter 23, pp. 456-476, at 456, Rule 23.01.

[62] See i.a. Rule 13 Tallinn Manual (2013), p. 54 ff; Rule 71 Tallinn Manual 2.0 (2017), p. 338 ff.
For an overview of indicative cyber operations, varying in form and intensity, see i.a. Gill, T.D., "Non-Intervention in the Cyber Context", Ziolkowski, K., [ed], *Peacetime regime for state activities in cyberspace*. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, pp. 21-237, at 234; Buchan, R., "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" in: 17 *Journal of Conflict & Security Law* (2012), no. 2, 212–227, at 211.

[63] Tallinn Manual 2.0 (2017), Rule 69, § 1, p. 331.

[64] See the statement by the Netherlands government: "The government believes that cyber operations can fall within the scope of the prohibition of the use of force, particularly when the effects of the operation are comparable to those of a conventional act of violence covered by the prohibition. In other words, the effects of the operation determine whether the prohibition applies, not the manner in which those effects are achieved.", in: *Parliamentary Papers II* (House of Representatives) 2018-2019, 33 649, no. 47, p. 8.
Also: The United Kingdom's Attorney General, *Cyber and International Law in the 21st Century* (Speech 23 May 2018), via < https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>.

[65] See e.g. the French statement, op. cit. note 42, p. 8: "To be categorised as an armed attack, a cyberattack must also have been perpetrated, directly or indirectly, by a State."

[66] See e.g. Gill and Ducheine, *op. cit.* note 22, p. 444: "It could also include a non kinetic attack amounting to a use of force, rising to the level of an armed attack, which resulted in more than nominal human casualties or significant physical damage or destruction to either military or civilian objects."

destruction of, property" would meet the scale and effects requirement,[67] though the "requisite degree of damage or injury remains, however, the subject of some disagreement".[68]

Apart from physical effects, it could be argued that a cyber operation directed against a State's critical infrastructure, provided the operation had the (potential) effect of seriously crippling a State's ability "to carry out and ensure the conducting of essential State functions or which severely undermine its economic, political and social stability for a prolonged period of time, even in the absence of human casualties and direct physical damage and destruction."[69] qualifies as an armed attack.[70]

The Netherlands accepted rather early, initially in general terms, the conclusions set forth in 'Cyber Warfare', a joint report by two advisory councils (CAVV and AIV).[71] The report stated that the "disruption of the state and/or society, or a sustained attempt thereto, and not merely an impediment to or delay in the normal performance of tasks" could indeed qualify as an armed attack. A mere "disruption of banking transactions or the hindrance of government activity", however, would not qualify as such. Notably, a cyber operation targeting "the entire financial system or prevents the government from carrying out essential tasks" could well be equated with an armed attack.[72]

Alongside others, the Netherlands' cabinet has now explicitly stated that it endorses the finding of the CAVV and the AIV that 'a cyber attack that has comparable consequences to an armed attack (fatalities, damage and destruction) can justify a response with cyber weapons or conventional weapons (...)'."[73] France stated that a "cyberattack could be categorised as an armed attack if it caused substantial loss of life or considerable physical or economic damage. That would be the case of an operation in cyberspace that caused a failure of critical infrastructure with significant consequences or consequences liable to paralyse whole swathes of the country's activity, trigger technological or ecological disasters and claim numerous victims."[74]

France's position is especially significant, as it, despite rejecting self-defence against non-state authors of attacks that cannot be attributed to a State in general terms, based its 2015 intervention against Da'esh / ISIS after the Bataclan attacks in November of that year exceptionally on self-defence.[75]

---

[67] Tallinn Manual 2.0 (2017), Rule 71, para. 7. Also: cyber strategies of several states, advance the view that a cyber attack which resulted in human casualties and/or significant physical damage qualifies as an armed attack justifying the exercise of self-defence. See e.g. U.S. Department of Defense, *Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011*, Section 934, November 2011, p. 4 available at <http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf>.

[68] Schmitt, M.N., "The Law of Cyber Warfare: Quo Vadis?", in: 25 *Stanford Law & Policy Review* (2014) 269-299, at 282.

[69] Gill and Ducheine, *op. cit.* note 22, p. 444.

[70] The International Group of Expert contributing to the Tallinn Manual was divided on this point. See Tallinn Manual (2013), Rule 13, Commentary - paragraphs 6-9.

[71] See *supra* note 5.

[72] See *supra* note 5, p. 21.

[73] *Parliamentary Papers II (House of Representatives)* 2018-2019, 33 649, no. 47, p. 8. Via <https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>.

[74] See *supra* note 42, p. 8.

[75] See *supra* note 42, p. 9.

Despite some States' positions,[76] it is still unclear whether cyber activities or operations that do not generate physical damage, destruction or injury may nevertheless qualify as an armed attack when they generate 'severe non-destructive or non-injurious consequences.' [77] State practice and *opinio juris* have yet to be developed regarding this subject. [78]

Despite the parlance used in the media and by members of the cyber community, in the "vast majority of cases, incidents referred to as a 'cyber attack' have not constituted a use of force, much less one rising to the threshold of an armed attack."[79] Examples such as the denial of service 'attacks' on Estonia (2007), defacements of websites in Georgia (2008) and examples of cyber espionage, sabotage and theft of data and intellectual property, cannot be seen as the use of force, nor an armed attack.[80] The arguable exception of a stand-alone cyber attack meeting the threshold requirements would be Operation Olympic Games[81] or Myrtus,[82] the operation against Iran's nuclear program (2008-2010) with the famous malware Stuxnet. The operation reportedly caused significant physical damage to the centrifuges engaged in the enhancement of nuclear material.[83] The Tallinn Manual group was unable to reach consensus on this point. However, with an eye to the 2015 and 2016 Ukrainian power outages, and thinking about societies' dependency on information, enabled by connectivity and electricity (or battery power), for instance during the current corona pandemic crisis, one would be hesitant to argue that international law, *jus ad bellum*, has reached its final status quo.

B. Mutual Cyber Defence?

As noted by Perot, is it obvious that a major cyber attack could either fit in the framework of the Solidarity Clause (Art. 222 EUTF), that is as a "terrorist attack", or in the framework of Article 42.7 EU Treaty, being "armed aggression" aka "armed attack".[84] In its 2013 Cyber Security Strategy, the EU however, states that "[a] particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause (Article 222 of the Treaty on the Functioning of the European Union)."[85] Interestingly, the strategy itself fails to refer to Article 42(7) of the Treaty on the European Union, containing the 'obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter' in case of 'armed aggression' (see above Section II). With Perot, other scholars nevertheless have signalled the possibility that cyber attacks could reach

[76] For an overview of (other) States that issued statements on international law in cyberspace, see i.a. <https://ccdcoe.org/library/strategy-and-governance/?category=intl-law-statements>.
[77] Schmitt, op. cit. note 68, p. 283, referring to the US position (described in: UN Doc. A/66/152, p. 18) and the Netherlands' stance (see supra note 73).
[78] Ducheine, op. cit. note 61, Rule 23.05, § 2, p. 473.
[79] Gill and Ducheine, op. cit. note 26, 458-459.
[80] For an overview, see e.g. Rid, T. "Cyber War Will Not Take Place", 35 *Journal of Strategic Studies* (2012), 1, 5-32.
[81] Sanger, Confront & Conceal, op. cit. 45.
[82] Rid, op. cit. note 80, at. 85.
[83] See e.g. Fidler, D.P., "Was Stuxnet an Act of War? Decoding a Cyberattack", in: 9 *Security & Privacy Magazine*, 4, 56-59; Gross, M.J., "A Declaration of Cyber-War", in: *Vanity Fair* (April 2011) at: <www.vanityfair.com/culture/features/2011/04/stuxnet-201104.print>.
[84] Perot, E., "The art of commitments: NATO, the EU, and the interplay between law and politics within Europe's collective defence architecture". In: European Security (2019) 28 (1), 40–65, at 46, via <http://www.tandfonline.com/doi/abs/10.1080/09662839.2019.1587746>.
[85] European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 7 February 2013, p. 19, via <https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf>]

the level of an "armed aggression" (aka "armed attack") and thus indeed trigger Art.42.7 TEU if these cyberattacks were to inflict serious damages to an EU member State.[86]

Regarding the Solidarity Clause (Art. 222 EUTF), the EU 'shall mobilise all the instruments at its disposal, including the military resources made available by the Member States' to counter certain threats, in particular terrorist, man-made or natural disasters. Noted by Roscini, the Solidarity Clause seems "broad enough to justify a coordinated military response in case of such new threats, which, according to the EU Cybersecurity Strategy , now also include 'particularly serious cyber incidents or attacks'.[87] In the meantime Article 42(7) is still applicable to cyber attacks that amount to "armed aggression" (or "armed attack").

In our view, it seems most likely that both the Solidarity Clause (Art.222 EUTF) and the Mutual Defence Clauses (Art. 42(7) EU Treaty) could be triggered by a cyber attack against a EU member State.[88]

Whether or not cyber attacks qualify as terrorist attack, a man-made disaster, or as armed aggression aka armed attack, will have to be seen. In any case, looking at recent incidents, it is rather obvious that cyber attacks play a relevant part in another threat to the security in and of the EU (member states) through the notion of hybrid threats. Demonstrated and researched by inter alia European Centre of Excellence for Countering Hybrid Threats (Helsinki, Finland),[89] the European Union's Institute for Security Studies,[90] and NATO's Strategic Communications Centre of Excellence (Riga, Latvia),[91] cyber operations in their various modalities are part of the so-called hybrid threat against the EU and its member States.

IV. Hybrid Threats and Mutual European Defence

As some authors[92] have pointed out, the term "hybrid warfare" may be an inappropriate term depending on the nature of the activities being described. Although "hybrid" has been defined in a variety of ways by a variety of authors, the approach taken by the European External Action Service[93] to "characterize" rather than define the concept appears to have quite some merit, given the wide diversity of the types of (hostile) activities subsumed under the overall concept. The use of hybrid tactics may involve the actual use of (military) force and as such be labelled "hybrid warfare," combining novel application of, or new methods regarding, (conventional means of) combat[94] with the other tactics associated with the concept of "hybrid." However, "hybrid" tactics without such use of military force are a threat in themselves as well and, as will be discussed below, since they are commonly intended to remain below the threshold of

---

[86] Roscini, M., *Cyber Operations and the Use of Force in International Law*. OUP Oxford, 2014, p. 97; Pawlak, P., *Cybersecurity and cyberdefence - EU solidarity and mutual defence clauses*. European Parliamentary Research Service, 2015via <http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/559488/EPRS_BRI(2015)559488_EN.pdf>; Fiott, D., *The Cybridisation of EU Defence*, EUISS, Alert 24, 2017, via <https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert 24 Cybridisation of defence.pdf>; Perot *op. cit.* note 84, at 46; Biscop, S., "The European Union and Mutual Assistance: More than Defence", in: *The International Spectator: Special Issue on the Responsibility to Protect* (2016) online 51 (2), 119–125. Via <http://www.tandfonline.com/doi/abs/10.1080/03932729.2016.1181453>.

[87] Roscini, *op. cit.* note 86.

[88] Roscini, *op. cit.* note 86.

[89] See <https://www.hybridcoe.fi/>.

[90] See <https://www.iss.europa.eu/tags/hybrid-threats>.

[91] See <https://www.stratcomcoe.org/>.

[92] See for example: Sari, *op. cit.* note 15, p. 450.

[93] EEAS, *Food-for-thought paper "Countering Hybrid Threats"*, EEAS(2015) 731.

[94] See, for example, Hoffmann, F.G., "Hybrid Warfare and Challenges," in *Joint Force Quarterly*, no. 52, 2009, especially pp. 36 – 37.

an armed attack they can raise questions regarding mutual defence and mutual assistance even without the addition of the concept of "warfare." Such situations do, however, raise questions regarding the legal basis for mutual response to such threats or activities.

A. The Status of Hybrid Threats as Armed Attack

Without seeking to duplicate definitions or descriptions readily available elsewhere, and not seeking to add new definitions to the ongoing discussions on hybrid threats, the following overview is merely meant as a summary in order to facilitate the discussion that follows. Briefly stated, hybrid threats consist of a combination of activities designed to undermine and weaken an opponent without resorting to conventional military attacks, at least at the outset. By exploiting inherent weaknesses in the opponent's organizational or societal structures and by employing a wide range of overt and covert tactics, the hybrid actor can disrupt and, as an essential element, both confuse the opponent and obfuscate the nature of the situation as well as the identity of the responsible actor. The activities involved may consist of (a combination of) disinformation and other forms of "information operations" to influence elections or otherwise undermine the authority and credibility of the local government, the use of cyberattacks either directly or through proxies to disrupt critical social processes or needs, seemingly random (but covertly coordinated) acts of terrorism or other criminal activities to disrupt or misdirect security forces, etc.[95]

Some hybrid threats, especially those combined with combat (and thus more accurately described as "hybrid warfare"), may be considered closely related to the more general category of irregular warfare and the sub-category thereof known as (counter-)insurgency. Although there is some degree of overlap between the types of activities and tactics in the context of hybrid threats and the tactics employed in the context of insurgencies,[96] there are differences between the two concepts. The United States Army defines "insurgency" as "the organized use of subversion and violence to seize, nullify, or challenge political control of a region,"[97] and certainly the use of subversion (and many of the tactics that may be applied towards that goal) could also fall under the category of "hybrid." Pouw offers an expanded definition of insurgency, stating that the term refers to:

> "a protracted, asymmetric and ideology-driven military-politico struggle that has crossed into an armed conflict and which is directed against the *status quo* within a State in order to bring about politico-strategic changes to address or alleviate certain causes, staged by organized networks composed of non-State actors whose conduct cannot be attributed to a State and which operate locally, nationally or trans-nationally."[98]

This more expanded and comprehensive definition is not only useful in its context of discussing (counter-)insurgency, but also in terms of delineating the difference between insurgency and hybrid threats and, in so doing, providing a basis for determining the status of hybrid threats in the context of the concepts of "armed attack" and national self-defence.

---

[95] EEAS, *op. cit.* note 93; Hoffmann, *op. cit.* note 94; Marović, J., "Wars of Ideas: Hybrid Warfare, Political Interference, and Disinformation," Carnegie Europe: https://carnegieeurope.eu/2019/11/28/wars-of-ideas-hybrid-warfare-political-interference-and-disinformation-pub-80419 (last accessed on 21 February, 2020).

[96] For a comprehensive discussion of (counter-)insurgency operations, see for example the United States Army, *Field Manual FM 3-24: Insurgencies and Countering Insurgencies*, available online at: https://fas.org/irp/doddir/army/fm3-24.pdf (last accessed on 21 February, 2020); and Pouw, E., *International Human Rights Law and the Law of Armed Conflict in the Context of Counter-Insurgency*, PhD Dissertation, University of Amsterdam, 2013, at <https://pure.uva.nl/ws/files/2243187/129355_thesis.pdf>.

[97] FM 3-24, *op. cit.* note 96, p. 1-2.

[98] Pouw, *op. cit.* note 96, p. 13.

The first difference concerns the generally accepted view that (counter-) insurgency is a form of irregular warfare and takes place in the context of a (non-international) armed conflict. Most modern hybrid threats, on the other hand, are intended, at least at the outset, to remain below the threshold and concomitant legal context of armed conflict. Secondly, both the United States Army and Pouw identify insurgencies as being related to causes espoused by the groups in question, normally referring to social, political or economic issues within the State in which the insurgency takes place. Hybrid threats, on the other hand, are more closely related, at least in the modern setting, to geopolitical ambitions and goals and are more inter-State in nature than intra-State. While the intra-State aspect already removes the basis for national self-defence in response to an armed attack, what is meant here is that modern hybrid threats are not generally related to a "fight for the good cause" in the sense of seeking to wage war, irregular or otherwise, to achieve idealistic goals but are instead a form of inter-State aggression aimed at rearranging the geopolitical balance in the favour of the aggressor through means (at least initially) short of war. Finally, while insurgencies are commonly carried out by non-State actors, hybrid threats are more commonly associated with State actors, notwithstanding the use of non-State proxies to frustrate or complicate attribution of the acts in question. While, as was stated above, both State actors and non-State actors can carry out an armed attack in the sense of Article 51 of the Charter of the United Nations and thus trigger the right of (collective) national self-defence, the difference to be pointed out here is that in the case of insurgencies, the non-State actors revert to irregular warfare as a result of the imbalance in war-fighting capacities compared to the State armed forces in question,[99] while in modern hybrid threats the State actor reverts to hybrid tactics in order to avoid triggering the right of national self-defence of the other State.

Both the brief description of hybrid threats given above and the discussion regarding the differences between hybrid threats and the concept of (counter-)insurgency lead to the clear conclusion that hybrid threats which do not involve combat in any case do not amount to an armed attack.[100] As regards hybrid threats which do involve combat, the criteria discussed in section II, above, would need to be applied in order to ascertain whether the threshold set forth in Article 51 of the Charter of the United Nations has been met. As not every use of force or form of aggression or (other) violation of international law constitutes an armed attack,[101] the question whether hybrid threats can trigger the right of national self-defence hinges on the nature of the activities involved. Given the activities generally considered indicative of modern hybrid threats, it would seem unlikely that, barring certain rare exceptions, such threats could be considered armed attacks. Consequently, the instances in which mutual defence in the sense of collective national self-defence would be possible under international law as a response to hybrid threats are rare at best, thus leading to questions regarding possible bases for mutual defence or mutual response by EU Member States against hybrid threats.

---

[99] FM 3-24, *op. cit.* note 96, p. 1-1.

[100] With the exception, of course, of the possibility of mounting a cyberattack that does meet the threshold of an armed attack in the context of a (wider) hybrid attack; see section III, above, for a discussion of cyberattacks in relation to the concept of armed attack.

[101] See, *inter multos alia*, Randelzhofer, A., "Article 2(4)" and "Article 51" in Simma, B. [ed.], *The Charter of the United Nations: A Commentary*, Oxford, 2nd ed., 2002; Klabbers, J., "Intervention, Armed Intervention, Armed Attack, Threat to the Peace, Act of Aggression, and Threat or Use of Force: What's the Difference?" in Weller, M. [ed.], *The Oxford Handbook of The Use of Force in International Law*, Oxford, 2015; Dinstein, *op. cit.* note 22, pp. 193 – 219.

B. Mutual Response to Hybrid Threats

Based on the observations above, exploring the options of mutual response by EU Member States against hybrid threats can be facilitated by breaking down the concept of hybrid threats into three categories. The first category consists of acts which, although clearly hostile and detrimental to the targeted State, do not involve the use of force or the deployment of military personnel (either overtly or covertly) onto the territory of the targeted State and are not intended as a precursor to invasion or other military use of force. This first category includes acts such as disinformation campaigns, the use of (social) media to undermine the legitimacy or authority of the government in question, cyberattacks below the threshold of an armed attack, influencing local elections, and the use of proxies to carry out disruptive or minor acts of terrorism or (other) criminal activities. The second category consists of the deployment of military forces onto the territory of the targeted State but without a prior armed attack. Although in itself legally an armed attack, such deployment without a prior "classic" armed attack may cause more significant political confusion as regards the appropriate response and the decision making surrounding such a situation than would a "normal" armed attack, in spite of the absence of any legal difference. The Russian annexation of the Crimean Peninsula referred to in the introduction would be a clear example of a situation falling within this second category. Note that activities in this category may be accompanied by activities from the first category and that the first category may be a prelude to the second category. Finally, the third category consists of the use of military force with "such scale and effects"[102] as to amount to an armed attack within the meaning of Article 51 of the Charter of the United Nations.

The first category defined above clearly provides the greatest challenge in terms of any response, mutual or solitary, by the targeted State. The acts constituting this category not only fail to meet the requirements for an armed attack, but also fall short of "aggression" as that term is defined in General Assembly Resolution 3314. This means that regardless of how one interprets the wording of Article 42.7 as discussed in Section II, above, the mutual defence clause cannot be invoked in response to hybrid threats in this first category. Moreover, the acts constituting this first category are of such a challenging nature in terms of responses against them that they may not warrant invocation of the solidarity clause in Article 222 TFEU either, depending on whether they could be classified as a "disaster." While terrorism is clearly included under Article 222 TFEU already by itself, and while the notion of "disaster" is broad and undefined and is now considered to include cyberattacks,[103] the (implementation of the) solidarity clause nonetheless requires a certain scale of impact that may not always be reached by individual acts from the first category of hybrid threats.[104] This means that responses to acts in this first category would primarily be the responsibility of the targeted State itself, although of course nothing in international law precludes a State from seeking the peaceful assistance, that is assistance without the use of force, from other States. For example, a State affected by

[102] ICJ, *Case Concerning Military and Paramilitary Activities In and Against Nicaragua* (Nicaragua vs. United States), Merits, 27 June 1986, paragraph 195.
[103] Joint Communication by the European Commission and the High Representative Of The European Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013)1, p. 19.
[104] Council Decision, *op. cit.* note 17, Article 3 under (a). Note that in addition to the "severe impact" requirement to qualify a situation as a "disaster," there is the additional requirement under Article 4 of the Decision that the situation is a "crisis" and that the State is overwhelmed by the crisis. To qualify as a crisis, the situation must, in accordance with Article 3 under (c), have "such a wide-ranging impact or political significance that it requires timely policy coordination and response at Union political level."

disinformation may ask other States to support its own counter-narratives in order to debunk the disinformation campaign. Similarly, a State suspecting (or accused of) irregularities in a local election may invite other States or international organizations to deploy neutral observers to monitor the elections. Finally, a State subject to hybrid threats in this first category may address the situation as a whole and bring it to the attention of the international community at large in order to demystify the situation. In other words, while an affected State may call on other States for assistance in response to acts which, essentially, can be considered breaches of sovereignty or intervention in the State's domestic affairs, the invocation of the solidarity clause would require the acts to be of sufficient gravity or sufficiently coherent to constitute a crisis and the invocation of the mutual defence clause would seem out of reach in this particular context. In other words, the assistance would be based on bilateral consultations and would be strictly voluntary, without the obligation set forth in Article 42.7.

Turning to the second category, the first observation regarding the acts in question is that they, in any case, fall under the definition of "aggression," given that Article 3 of Resolution 3314 does not require the actual use of force in connection with an invasion, occupation or annexation by the armed forces of the aggressor State. This means that a military invasion or occupation which was rendered possible as a result of hybrid acts from the first category (and may be combined with such acts) qualifies as "aggression" as well as qualifying as an armed attack from a legal point of view. That means that as regards political decision making, a choice is available regarding this category between the broader label of "aggression" and the specific label of "armed attack." Such differentiation would be more theoretical and political rather than legal and the wording of Article 42.7 raises the question whether such political creativity would absolve the states in question from their obligation to assist the affected state. This category then clearly relates to the discussion in Section II, above, regarding the legal meaning of the terminology of Article 42.7 as regards "armed aggression" and whether that terminology has a broader meaning than "armed attack" as used in Article 51 of the Charter of the United Nations. As discussed above, the history of the clause and the specific reference to Article 51 in Article 42.7 appear to favour what Sari refers to as the "narrow interpretation,"[105] which also appears to be the interpretation of the clause supported by Thym,[106] and limits the meaning of Article 42.7 to the notion of an armed attack as also used in Article 51 UNCH and Article 5 of the North Atlantic Treaty. On the other hand, Sari provides a convincing argument that the phrase "armed aggression" was deliberately left in the treaty even after suggestions were made to change it, and considers both the narrow interpretation and a wider approach to be "tenable."[107] Finally, the Clingendael report on "Spearheading European Defence" clearly embraces the wider approach and unequivocally states that the clause "covers a wider category of threats than NATO's Article 5," pointing out that contrary to Article 5 of the North Atlantic Treaty, Article 42.7 "makes reference to the broader category of 'armed aggression'."[108] Much will consequently depend on the outcomes of the ongoing discussions within the EU regarding the operationalisation of Article 42.7 and the choices to

[105] Sari, *op. cit.* note 15, pp. 417 – 418.
[106] Fischer & Thym, *op. cit.* note 10, p. 1225. Note, however, that Thym also states that this interpretation does not necessarily clarify the issue, as he considers the threshold for the use of force in national self-defence to be "disputed in public international law."
[107] Sari, *op. cit.* note 15, pp. 418 – 419.
[108] Bakker (et al.), *op. cit.* note 19, p. 25. However, given the definition of aggression in United Nations General Assembly resolution 3314 (XXIX) and the generally accepted interpretation of "armed attack" it remains unclear which acts of *armed* aggression would then be included in this broader scope that do not constitute an armed attack in the narrow interpretation of the clause.

be made therein by the Member States regarding the scope of the clause. Should the outcome of those discussions favour the broader interpretation of Article 42.7, then clearly the clause could be invoked in response to hybrid threats in this second category.[109] While the mutual response following such invocation must, of course, comply with international law and may differ from the mutual response following an armed attack,[110] a broad interpretation of Article 42.7 and its application in response to hybrid threats in this second category would in any case allow (mandatory) mutual EU response.

The third and final category would appear to pose the least conceptual challenges as regards its relationship with Article 42.7. Clearly hybrid attacks[111] amounting to armed attacks in the sense of Article 51 of the Charter of the United Nations would fall within the scope of the mutual defence clause and would justify invoking that clause, regardless of the discussion regarding possible broader application of the clause. Given the scope and nature of an armed attack and the resultant military confrontation and ensuing armed conflict, it would also seem likely that such a situation would be addressed purely by the Member States and would thus fall outside the scope and purpose of the solidarity clause. Such a situation would, of course, also allow those Member States which are also NATO Member States a choice as to whether to invoke Article 42.7 of the TEU, or Article 5 of the North Atlantic Treaty.

In conclusion, placing the categories of hybrid attacks discussed above in a matrix, the following response options and coordinating mechanisms would apply:

[109] Given the scope and impact of hostile military incursions, occupations, etc., clearly Article 222 TFEU could be invoked as well, with the concomitant roles and responsibilities for the EU institutions.

[110] Note that the Netherlands recognizes an invitation by another State to deploy military forces and to use force in conformity with (international) law on the territory of the inviting State as a legal basis under international law and that this legal basis is separate from the right to collective national self-defence (Parliamentary Document 29521 no. 41, p. 7). Regardless of whether the acts under discussion constitute an armed attack and regardless of any response on the basis of national self-defence, it would seem at least likely that the affected State would (or would at least be legally justified to) invite other Member States to provide assistance on this basis even without any recourse to Article 42.7.

[111] Note that the discussion of category 3 includes not only hybrid attacks which meet the criteria for an armed attack by themselves, but also hybrid attacks which meet the criteria for the "accumulation of events" theory.

Category	Nature of threat	Response options	Coordinated by
1.a.	Acts not including the use of armed force or deployment of invading or occupying forces and not rising to the level of a disaster or crisis	Invitation by affected State	Affected State bilaterally
1.b.	Acts not including the use of armed force or deployment of invading or occupying forces, rising to the level of a disaster and crisis and overwhelming the national resources	(1) Invitation by affected State (2) Article 222 TFEU	(1) Affected State bilaterally (2) Council, Commission and HR
2.	Acts not rising to the level of an armed attack but including the deployment of invading or occupying forces	(1) Invitation by affected State (2) Article 222 TFEU (3) Article 42.7 TEU in broad interpretation	(1) Affected State bilaterally (2) Council, Commission and HR (3) Affected State bilaterally
3.	Acts rising to the level of an armed attack	(1) Invitation by affected State (2) Article 42.7 TEU	(1) and (2) Affected State bilaterally

V. Conclusion

The mutual defence clause set forth in Article 42.7 of the Treaty on European Union is a much-debated provision that is notoriously vague as regards its precise scope, especially regarding the trigger criteria for invoking the clause by the Member States. Although similar to Article 5 of the North Atlantic Treaty, and similarly having been invoked only once, the wording of the clause leaves room for interpreting it in either a much broader way than the NATO version would allow, or in a narrow interpretation similar to the NATO version and in keeping with the heritage of the clause in Article V of the modified Brussels Treaty establishing the WEU. Although the narrow version would appear more accurate in terms of that heritage and in light of the arguments presented in Section II, above, the debate as to the precise meaning and scope of the provision has not been settled yet and is currently being held both in the academic world and in the political deliberations between the EU Member States in the context of exploring the operationalisation of Article 42.7. Consequently, no definitive conclusion as to the precise scope of the provision can be provided in this chapter.

What is clear, however, is that the application of the provision must, of course, comply with the rest of public international law and that the provision contains at least some overlap with the solidarity clause in Article 222 of the Treaty on the Functioning of the European Union. This means that invoking the mutual defence clause must, *inter alia*, comply with the criteria established on the basis of Article 51 of the Charter of the United Nations and that any invocation of the clause outside the realms of collective self-defence against an armed attack

may be subject to limitations as to the precise nature of the mutual response.[112] Furthermore, in situations which can be categorized either as "armed aggression," leaving aside the question as to the precise scope of that concept, or as a "disaster" and "crisis" as defined by Council Decision 2014/415/EU, Member States must choose whether to address the situation at hand through bilateral consultations or by transferring coordination duties and responsibilities to the EU institutions. Apart from any legal considerations in that regard, the invocation of the clause by France in response to large-scale terrorist attacks – a prime example of a situation that would overlap both provisions – would seem to suggest that the choice as to which provision will be invoked will ultimately be a political one.

As regards the relationship between Article 42.7 and cyberattacks, departing from the position that "armed aggression" in Article 42.7 EU Treaty reads as "armed attack" in the meaning of the UN Charter, it is clear that the classic interpretation of an armed attack, complicated as it is, has been affected by the terrorist attacks in the United States (2001, '9/11') and France (2015, Bataclan). It is now clear that armed attacks may be launched with non-military means, e.g. cyber weapons, by both state and non-state actors. According to some states (and scholars), a series of smaller scale uses of force could constitute, what is in effect, a phased armed attack. Noting the dependencies of economies and societies on cyberspace, launching cyber operations that potentially equal the effects of an armed attack, as was the case on 9/11, in not just a theoretical chance or risk. A number of European states (France, the Netherlands) and the United Kingdom have advanced the view that a cyber operation could be categorised as an armed attack if it caused substantial loss of life or result in considerable physical or economic damage, through for instance, a failure of critical infrastructure or parts of society.

As regards the relationship between Article 42.7 and hybrid threats, the discussion in Section IV, above, explored the nature of hybrid threats as an armed attack and the options as regards mutual response by EU Member States against hybrid threats. From that discussion, it can be concluded that the scope of the concept of hybrid threats and the diverse nature of the acts in question do not allow a singular categorization of the response against such threats. In terms of mutual defence, the nature of modern hybrid threats as intended to obfuscate the reality of the situation and to render attribution more difficult, if not impossible at least at first, further complicates the issue. Applying a categorisation to the concept of hybrid threats, however, it becomes clear that only those hybrid threats which qualify as an armed attack unequivocally allow invocation of Article 42.7. Hybrid threats which qualify as "aggression" (or even "armed aggression") as defined in United Nations General Assembly Resolution 3314 (XXIX) but which do not rise to the level of an armed attack would allow invocation of Article 42.7 if the "broad interpretation" is applied. However, the mutual response against such threats may then be limited by the other elements of public international law governing the use of force in inter-State relations. Furthermore, such threats may also warrant invoking the solidarity clause if the political will to do so exists and if the State in question is willing to seek the assistance of the EU institutions. Finally, hybrid threats not rising to the level of (armed) aggression may allow invocation of the solidarity clause if the scope and impact are of sufficient gravity, but fall well below even a broadly interpreted threshold for invoking Article 42.7. Since, however, these observations are made from a purely legal and academic point of view, however, it remains to

[112] Of course the additional requirements under the Charter and international law apply as well, such as notifying the Security Council (and accepting an end to the right of self-defence if the Council takes the necessary measures to maintain international peace and security) and applying the principles of necessity and proportionality.

be seen how the Member States will consider the relationship between hybrid threats and the mutual defence clause in their deliberations on operationalising the clause.