Dialects: collective cyber defence in the EU and NATO

Pijpers, P.B.M.J.; Boddens Hosang, H.; Ducheine, P.A.L.

DOI
10.2815/57567

Publication date
2022

Document Version
Final published version

Published in
A language of power?

euiss European Union Institute for Security Studies

A LANGUAGE OF POWER?

Cyber defence in the European Union

Edited by
Patryk Pawlak and François Delerue

With contributions from
Hans Boddens Hosang, Raluca Csernatoni, Paul A.L. Ducheine, Aude Géry, Laurent Gisel, Mika Kerttunen, Kubo Mačák, Antonio Missiroli, Peter B.M.J. Pijpers, Matthias Schulze, Eneken Tikk

The EUISS is an agency of the European Union

CHAILLOT PAPER / 176
November 2022

European Union Institute for Security Studies (EUISS)

100, avenue de Suffren
75015 Paris

http://www.iss.europa.eu
Director: Gustav Lindstrom

print	ISBN 978-92-9462-143-6	online	ISBN 978-92-9462-142-9
	CATALOGUE NUMBER QN-AA-22-004-EN-C		CATALOGUE NUMBER QN-AA-22-004-EN-N
	ISSN 1017-7566		ISSN 1683-4917
	DOI 10.2815/067862		DOI 10.2815/57567

Published by the EU Institute for Security Studies and printed.
Luxembourg: Publications Office of the European Union, 2023.
Cover image credit: Pawel Czerwinski/Unsplash

European Union
Institute for Security Studies

A LANGUAGE OF POWER?

Cyber defence in the European Union

Edited by
Patryk Pawlak and François Delerue

With contributions from
Hans Boddens Hosang, Raluca Csernatoni,
Paul A.L. Ducheine, Aude Géry, Laurent Gisel,
Mika Kerttunen, Kubo Mačák, Antonio Missiroli,
Peter B.M.J. Pijpers, Matthias Schulze, Eneken Tikk

The EUISS is an agency
of the European Union

CHAILLOT PAPER / 176
November 2022

CHAPTER 7

DIALECTS: COLLECTIVE CYBER DEFENCE IN THE EU AND NATO

by
PETER B.M.J. PIJPERS, HANS BODDENS HOSANG AND PAUL A.L. DUCHEINE

INTRODUCTION

Collective defence is the cornerstone of the North Atlantic defence system, in which the European partners rely heavily on the (nuclear) deterrence assets of the United States. The solidarity in this system has been relatively one-sided. Given the US shift to the Pacific [(1)], in a geopolitical context where threats against the core values of the EU remain acute or have even magnified [(2)], the European Union is pursuing increased strategic autonomy [(3)].

The EU nowadays has a clause for mutual defence similar to NATO's Article 5, replacing the somewhat obsolete collective defence system of the Western European Union (WEU) [(4)]. So far, both NATO's Article 5 and the EU's mutual defence clause have been invoked only once, in the latter case by France in search of political rather than military support [(5)]. Though the collective defence systems of both the EU and NATO are built on the customary international law standard regarding the right of self-defence [(6)], the wording and the scope of the clauses differ. Whereas NATO is confined to the military sphere and a nascent diplomatic role, to the EU all instruments of power – such as the economy, diplomacy, information, culture, knowledge [(7)] – are available.

(1) Manyin, M.E. et al, 'Pivot to the Pacific? The Obama Administration's "rebalancing" toward Asia', CRS Report for Congress, 2012 (https://sgp.fas.org/crs/natsec/R42448.pdf).

(2) NATO, 'Madrid Summit Declaration 29 June 2022', NATO Press Release. Bullet 3, 29 June 2022 (https://www.nato.int/cps/en/natohq/official_texts_196951.htm); Johnson, R., 'The first phase of the Russian invasion of Ukraine 2022', Changing Character of War Centre, Oxford, 2022.

(3) Sari, A., 'Mutual Assistance Clauses of the North Atlantic and EU Treaties', *10 Harvard National Security Journal*, 2019, p. 408; EU High Representative for Foreign Affairs and Security Policy, 'Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy', 2016 (https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf).

(4) Boddens Hosang, J.F.R. and Ducheine, P.A.L, 'Implementing Article 42.7 of the Treaty on European Union: Legal foundations for multual defence in the face of modern threats', ACIL, 2020, pp. 3-4 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748392).

(5) Bakker, A. et al., 'The EU's mutual assistance clause' in *Spearheading European Defence: Employing the Lisbon Treaty for a stronger CSDP,* Clingendael Institute, 2016 (https://www.clingendael.org/sites/default/files/2016-02/Report_Spearheading_European_Defence.pdf).

(6) As laid down in Article 51 of the Charter of the United Nations.

(7) Ducheine, P.A.L. and Pijpers, P. B.M.J., 'The missing component in deterrence theory: The legal framework' in Osinga, F.P.B. and Sweijs, T. (eds), *Deterrence in the 21st Century – Insights from Theory and Practice* Springer, 2021, pp. 481-482.

The differences between the EU and NATO collective defence systems come into sharper focus with regard to their ability to cope with threats emerging from cyber operations. In cyberspace, state and non-state actors can operate on a near equal footing; moreover, although prone to generate strife and even conflict, activities in cyberspace predominantly fall below the threshold of the use of force, hence outside the classic military remit.

The problem that emerges is that cyberattacks (below the level of force) and collective defence systems (against an armed attack) appear to be mutually exclusive. Is collective cyber defence an oxymoron or should the mechanism be revisited, embracing a broader vision of collective defence? And if so, given the fact that the EU has a wide array of instruments of power at its disposal (from diplomatic measures via economic sanctions and financial fines to legal retorsions) would this then also imply that the EU is better equipped to provide a security umbrella against modern cyber threats?

This chapter aims to offer a strategic and legal perspective on collective defence against cyberattacks in an EU and NATO context. In order to assess whether the EU is better equipped than NATO to provide a collective defence system against cyberattacks, first various types of cyberattacks including their core attributes will be described. Next, a comparative overview of the NATO and EU collective defence systems is presented. In the following section the attributes of cyberattacks are cross-referenced with the collective defence systems to see what gaps remain. In the final section some concluding reflections are provided and an answer to whether or not the EU is suited to provide a collective cyber defence system.

ON CYBER OPERATIONS

Collective defence is associated with armed attack in the traditional land, sea or maritime domains. Cyberattacks differ from traditional kinetic attacks in several ways. To put the differences into context a short description of cyberspace and the various categories of malicious cyber operations is provided in this section.

Cyberspace is a domain in which activities are performed and carried out, similar to the land, sea, space or air domains [(8)]. Therefore, cyberspace is not an instrument or a weapon as such, but rather 'an enabling environment that allows actors to transmit information to large audiences at low cost, near instantaneously, through multiple distribution points, across borders and with heightened opportunities for anonymity' [(9)]. Cyberspace is an operational domain contained within the information environment. The information environment entails three conceptual dimensions: the cognitive, virtual and physical [(10)]. These can in turn be subdivided into seven layers as depicted in the diagram opposite.

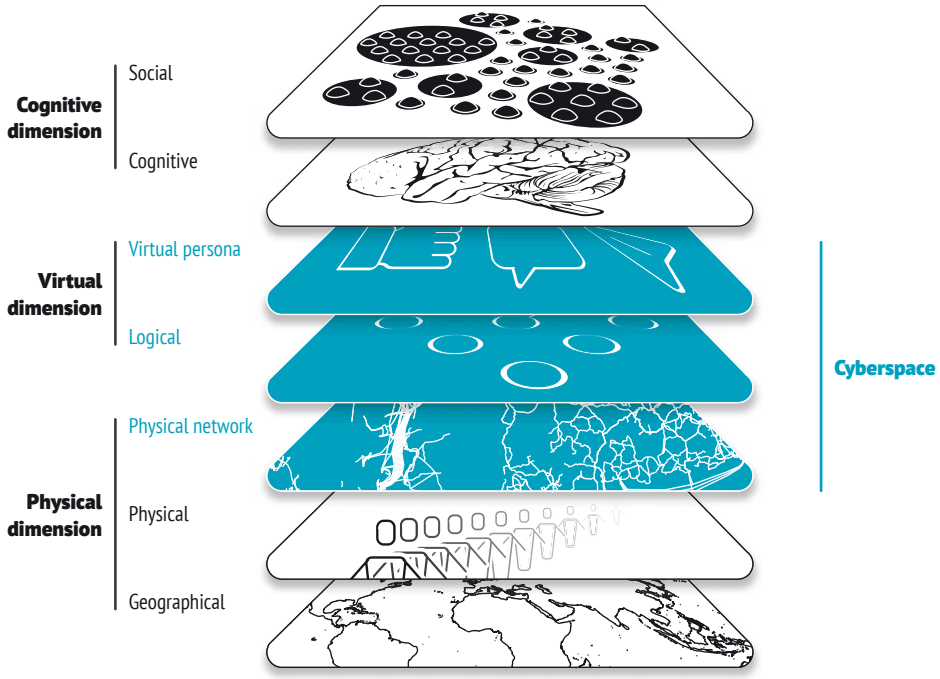
For the purpose of this chapter, the scope of cyberspace consists of three layers: (i) the physical network layer of the computers,

(8) Heintschel von Heinegg, W., 'Territorial sovereignty and neutrality in cyberspace', US Naval War College, *International Law Studies*, Vol. 89, 2013, p. 123; Nye, J. S. Jnr, 'Cyber Power', Harvard Kennedy School, Belfer Centre for Science and International Affairs, May 2010, p.7 (https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf); Delerue, F., 'Reinterpretation or contestation of International Law in cyberspace?', *Israel Law Review*, Vol. 52, No 3, November 2019, pp. 304-305.

(9) Lin, H.S. and Kerr, J., 'On cyber-enabled information warfare and information operations', in Cornish, P. (ed.), *Oxford Handbook of Cybersecurity*, 2021, pp. 262–265; Jensen, E., 'Cyber sovereignty: The way ahead', *Texas International Law Journal*, Vol. 50, No 2, 2015, p. 275, p. 279.

(10) Ducheine, P.A.L., van Haaster, J. and van Harskamp, R., 'Manoeuvring and generating effects in the information environment' in Ducheine, P.A.L and Osinga, F.P.B (eds.), *Winning Without Killing: the strategic and operational utility of non-kinetic capabilities in crisis - NL ARMS 2017*, 2017, pp. 5-7; CJCS, 'Information Operations - Joint Publication 3-13', Washington D.C., 2014, p. I.1.

The infomation environment and cyberspace



Data: Data: Ducheine, P.A.L. et al (eds.), *Winning Without Killing: the strategic and operational utility of non-kinetic capabilities in crisis*, 2017; van Haaster, J., *On Cyber: The utility of military cyber operations during armed conflict*, 2018.

cables and hubs, i.e. the hardware storing data and making the transfer of data possible; (ii) the logical layer of data, software applications and protocols [11]; and (iii) the cyber-persona layer which consists of virtualised representations of entities or groups and enables them to access the logical layer and hardware, and thus to interact in cyberspace (*inter alia* on the internet and social media).

With the inception of cyberspace three new layers have been introduced for human communication, commerce but also conflict as we have seen with the 2010 Stuxnet attack [12], the hack-and-release activities during the 2016 US presidential election [13], or more recently the SolarWinds hack compromising critical infrastructure [14], affecting the cognitive and physical layers of the information environment [15].

Activities in cyberspace can be divided into so-called 'hard' and 'soft' cyber operations [16]. Hard cyber operations are cyber-related

(11) The internet entails the physical network layer and the logical layer. See *On Cyber*, op.cit., pp. 136-137.

(12) Lindsay, J.R., 'Stuxnet and the limits of cyber warfare', *Security Studies*, Vol. 22, 2013, pp. 378-389, p. 365,

(13) Office of the Director of National Intelligence, 'Assessing Russian activities and intentions in recent US elections', Washington, 2017 (https://www.dni.gov/files/documents/ICA_2017_01.pdf).

(14) Singh, P., 'SolarWinds: Cyber strategists are back to the drawing board', *Hindustan Times*, 27 December 2020 (https://www.hindustantimes.com/analysis/solarwinds-cyber-strategists-are-back-to-the-drawing-board/story-L5QunVMY7vRa04isQlT1QL.html).

(15) Betz, D.J. and Stevens, T., 'Power and Cyberspace', *Adelphi Series*, Vol. 51, No 424, 2011, p. 35, p. 41.

(16) Pijpers, P. B.M.J and Arnold, K.L., 'Conquering the invisible battleground', *Atlantisch Perspectief*, Vol. 4, No 44, 2020, pp. 12-14; Ducheine, P.A.L. and van Haaster, J., 'Fighting power, targeting and cyber operations' International Conference on Cyber Conflict, CYCON 303, 2014, p. 313; Ducheine, P.A.L. and Pijpers, P. B.M.J., 'The notion of cyber operations' in Tsagourias, N. and Buchan, R. (eds), *Research Handbook on International Law and Cyberspace*, 2nd edition, Edward Elgar, 2021.

activities *in* cyberspace such as hacking a computer or disabling, disrupting or destroying software [17] or virtual persona [18]. Hard cyber operations affect cyberspace, while soft cyber operations are cyber-related activities that use cyberspace as a vector. Soft cyber operations use cyberspace as a vector to 'weaponise' the content of a message but also manipulate the source (or outlet) of the message (including via falsifying social media accounts) [19] to influence the cognitive dimension of other actors [20].

Contrary to traditional kinetic attacks, cyberattacks are remotely executed operations that predominantly take place below the threshold of an armed attack as envisioned in Article 51 of the UN Charter [21]. When cyberattacks take place, it is often not the malign act (emplacing malware) that will be noticed, but the effects of it, which may develop (much) later in time [22]. Moreover, given the relatively low costs of entry, attacks may often be perpetrated by non-state actors that may not be under control of a state [23]. Since the impact of cyberattacks, especially in soft cyber operations, is often less tangible, it is generally considered that it is more difficult to attribute the attack to a specific actor [24]. The so-called attribution problem in cyberspace [25] must not be overexaggerated however. The attribution process entails a technical [26], legal and political layer. The layers are not necessarily interrelated, an act can be attributed for political reasons [27] without providing technical evidence [28]. And, finally, even if aggressive acts can be attributed to an actor, an attack carried out in or via the virtual dimension of cyberspace (e.g. related to iCloud services or email-accounts) cannot always be traced to a specific territory, which could have legal implications [29].

(17) Castro, S., 'Towards the development of a rationalist cyber conflict theory', *The Cyber Defense Review*, Vol. 6, No 1, Winter 2021, p. 38 (https://cyberdefensereview.army.mil/Portals/6/Documents/2021_winter_cdr/03_CDR_V6N1_Castro.pdf).

(18) 'Manoeuvring and generating effects in the information environment', op.cit., pp. 2 & 15; Kello, L., *The Virtual Weapon and International Order*, Yale University Press, New Haven, 2017, pp. 51-53; 'Cyber Power', op.cit., p. 6.

(19) Shires, J., 'Hack-and-leak operations: Intrusion and influence in the Gulf', *Journal of Cyber Policy*, Vol. 4, No 2, 2019, p. 240; 'Cyber Power', op.cit., pp. 2 and 5.

(20) Cyber-related influence operations are inherently soft cyber operations. see: Stephens, D., 'Influence operations & international law', *Journal of Information Warfare*, Vol.19, No 4, 2020, p. 2.

(21) Gill, T.G. and Ducheine, P.A.L, 'Anticipatory self-defense in the cyber context', *International Law Studies*, Vol. 89, Naval War College, 2013, p. 459.

(22) Mueller, R.S., 'Report on the investigation into Russian interference in the 2016 presidential election', Volume 1 of II, US Department of Justice, Washington D.C., March 2019, pp. 38-40.

(23) Merrigan, E., 'Blurred lines between state and non-state actors', Council on Foreign Affairs, 2020 (https://www.cfr.org/blog/blurred-lines-between-state-and-non-state-actors).

(24) Finlay, L. and Payne, C., 'The attribution problem and cyber armed attacks', *AJIL Unbound 202*, Vol.113, 2019, pp. 203-205.

(25) Dipert, R.R., 'The ethics of cyberwarfare', *Journal of Military Ethics*, Vol. 9, 2010, p. 385.

(26) Tsagourias, N. and Farrell, M., 'Cyber attribution: Technical and legal approaches and challenges', *European Journal of International Law*, Vol. 31, No 3, 2020, pp. 947-951.

(27) Finnemore, M. and Hollis, D.B., 'Beyond naming and shaming: Accusations and International Law in cybersecurity', *European Journal of International Law*, Vol. 31, No 3, August 2020, pp. 1002-1003.

(28) Some states argue that there is no obligation to disclose the evidence for (political) attribution, see: Eichensehr, K., 'Cyberattack attribution and international law', *Just Security*, 2020 (https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law/); Egan, B., 'International Law and stability in cyberspace', *Berkeley Journal of International Law*, Vol. 35, No 1, 2016 (https://www.law.berkeley.edu/wp-content/uploads/2016/12/BJIL-article-International-Law-and-Stability-in-Cyberspace.pdf); Ministère des Armées, 'Droit international appliqué aux opérations dans le cyberespace', 2019, pp. 10-11 (https://www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf).

(29) Pijpers, P. B.M.J. and Van Den Bosch, B.G.L.C, 'The "virtual Eichmann": On sovereignty in cyberspace', ACIL Research Paper 2020-65, December 2020, pp. 19-20 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3746843).

COLLECTIVE DEFENCE IN AN EU AND NATO CONTEXT

The right of states to defend themselves against an armed attack is an inherent right deriving from the very nature of statehood [30]. This rule of customary international law is also recognised in Article 51 of the UN Charter [31], and guided by the principles of necessity, proportionality and immediacy [32]. The inherent right of self-defence relates to a response to an (imminent) armed attack, in which case the use of force is permitted, thereby exempting *jus cogens* on the prohibition of the use of force [33], and Article 2(4) of the UN Charter.

The right of self-defence can be exercised individually or collectively as stipulated in NATO's collective defence clause of Article 5 of the North Atlantic Treaty [34], and in the EU's mutual assistance (or mutual defence) clause of Article 42(7) [35] of the Treaty on European Union (TEU). Aside from an assistance clause, the Member States of the EU can also invoke a solidarity clause (Article 222 Treaty on the Functioning of the EU (TFEU) in case of terrorist attacks or natural and man-made disasters [36].

The mutual defence clauses of the EU and NATO both refer to Article 51 of the UN Charter and are similar in intent, although differing in substance. Taking also the EU solidarity clause into account, the differences relate to the activation criterion, the territorial scope and binding nature of the clause, and the arrangements for implementation [37].

The *casus foederis* or the trigger for invoking NATO's Article 5 is an 'armed attack' echoing the words of Article 51 of the UN Charter. The mutual assistance clause of the EU uses the term 'armed aggression' [38]. Despite linguistic differences, the factual differences are marginal. [39] One explanation for the differences is that 'armed aggression' was translated literally from the French version of Article 51 UN Charter, which refers to *agression armée* instead of armed attack [40]. In the view of one expert, this is the narrow interpretation of the activation criterion, equating armed

[30] Boddens Hosang, J.F.R., *Rules of Engagement and the International Law of Military Operations*, Oxford Monographs in International Humanitarian and Criminal Law, Oxford University Press, Oxford, 2020, pp. 51–53.

[31] 'Anticipatory self-defense in the cyber context', op.cit., pp. 441–443.

[32] *Legality of the Threat or Use of Nuclear Weapons – Advisory Opinion of 8 July 1996* [1996], ICJ Reports, Paras 40–42; 'Anticipatory self-defense in the cyber context', pp. 448–452.

[33] *Case Concerning Military and Paramilitary Activities in and against Nicaragua* [1986], ICJ Reports, Para 190.

[34] 'Article 5: 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. (…).', North Atlantic Treaty, 1949 (https://www.nato.int/cps/en/natolive/official_texts_17120.htm).

[35] Article 42(7): 'If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States. Commitments and cooperation in this area shall be consistent with commitments under the North Atlantic Treaty Organisation, which, for those States which are members of it, remains the foundation of their collective defence and the forum for its implementation.' *Consolidated Version of the Treaty on European Union*, *O J* C–326, 2012. (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A12008M042).

[36] NATO could refer to Article 4 when 'territorial integrity, political independence or security of any of the Parties is threatened'. This article will not be dealt with in this chapter since it does not imply collective action of the alliance. See: North Atlantic Treaty, Article 4.

[37] Pawlak, P., 'Cybersecurity and cyberdefence: EU solidarity and mutual defence clauses', EPRS Briefing, June 2015 (https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/559488/EPRS_BRI(2015)559488_EN.pdf).

[38] Though it is a restatement of the commitments laid down in Article 5 of the Treaty of Brussels that established the Western European Union. See 'Mutual Assistance Clauses of the North Atlantic and EU Treaties', op.cit., p. 433.

[39] 'Implementing Article 42.7 of the Treaty on European Union', op.cit., p. 7.

[40] Perot, E., 'The art of commitments: NATO, the EU, and the interplay between law and politics within Europe's Collective Defence Architecture', *European Security*, Vol. 28, No 1, 2019, pp. 45–46.

aggression to armed attack, while a broader interpretation would give room for providing assistance in a case where unlawful force is used 'that does not reach the gravity threshold of an armed attack' [41]. He argues that it is not likely that the drafters intended to broaden the notion of armed attack, but the possibility must not be discarded completely [42]. This rationale can be supported by arguing that the EU intended to apply alternative collective security mechanisms, by offering the option of assistance based on solidarity in cases other than an armed attack via Article 222 TFEU.

Both NATO and EU mutual defence clauses have a territorial scope [43] and refer to attacks on the territory of the Member States. NATO includes extraterritorial military assets within the region demarcated by Article 6 of the North Atlantic Treaty but excludes overseas territories (e.g. Dutch or French Antilles) [44]. The EU, on the other hand, includes the latter [45]. The EU solidarity clause also relates to territory but to a lesser extent, meaning that the EU could, in reference to Article 222 TFEU, still request assistance for disasters befalling military forces or embassies located outside the EU.

The Member States of NATO and the EU are required to provide support in the event that the collective defence clause is invoked, but the obligatory nature of the clauses differ. While Article 42(7) TEU uses stronger language, it cannot address all Member States equally due to the neutrality of some of them [46]. NATO does not require the Member States to provide aid and assistance 'by all the means in their power' as Article 42(7) requests but asks for such action as the Member States deem necessary. A bigger difference, however, concerns the exact nature of the assistance [47]. In both the EU and NATO, Member States can use all instruments of power to respond, including – but not limited to – the use of force [48]. However, the contribution of NATO Member States is, or can be, substantial in military terms [49], while the EU contribution might not go beyond political and diplomatic support [50].

Invoking Article 222 TFEU in the event of a terrorist attack or a disaster will result in an EU-led and embedded activity [51], while Article 42(7) TEU or Article 5 of the NATO Treaty 'entail direct state-to-state assistance without explicitly mentioning any role for the common EU or NATO institutions as such' [52]. The reason for this is that Articles 42(7) TEU and Article 5 NATO Treaty derive from the inherent right of self-defence, while Article 222 TFEU does not.

---

(41) 'Mutual Assistance Clauses of the North Atlantic and EU Treaties', op.cit., pp. 417-418.

(42) Ibid, p. 419.

(43) 'The art of commitments', op.cit., pp. 49-50.

(44) North Atlantic Treaty, op. cit., Article 6. Although Article 4 of the NATO Treaty has a world-wide scope. Bumgardner, S.L., 'Article 4 of the North Atlantic Treaty', *Emory International Law Review*, Vol. 34, 2019, p. 76.

(45) 'The art of commitments', op.cit., (n 268), p. 49.

(46) 'Mutual Assistance Clauses of the North Atlantic and EU Treaties', op.cit., p. 435.

(47) 'The EU's mutual assistance clause', op.cit., p. 25; 'Implementing Article 42.7 of the Treaty on European Union', op.cit., p. 7.

(48) 'The art of commitments', op.cit., p. 53.

(49) Ibid, p. 51. Moreover, the TEU will not overrule the obligations as laid down in the NATO treaty. Art 42.7 TEU [5] states that 'Commitments and cooperation in this area shall be consistent with commitments under the North Atlantic Treaty Organisation, which, for those States which are members of it, remains the foundation of their collective defence and the forum for its implementation.'

(50) When France invoked Article 42(7) in 2015 it shifted military power from out-of-area operations to mainland France. Other EU Member States have, in response, taken over some of those out-of-area tasks, which could also be valued as an act of solidarity. ECFR, 'Article 42.7: An Explainer', European Council on Foreign Relations, 2015 (cfr.eu/article/commentary_article_427_an_explainer5019/).

(51) Council of the European Union, 'Decision on the arrangements for the implementation by the Union of the solidarity clause', *Official Journal of the European Union*, L 192 53, Article 3 (c) jo Article 5, 2014, pp. 56-57; Article 222 TFEU speaks about 'the Union and its Member States', while Article 42(7) TEU solely addresses the Member States.

(52) 'The art of commitments', op.cit., p. 52.

COLLECTIVE CYBER DEFENCE

The notion of a collective defence system presents challenges and is never free from political considerations. NATO has acted in a collective and concerted manner during many operations since its inception in 1949, and Article 5 was never invoked in the Cold War era. Kinetic operations, and the subsequent use of the collective defence system [53], became even more complex with the rise of terrorism. The attacks by a non-state actor on the Twin Towers and the Pentagon on 11 September 2001 paradoxically triggered the invocation of Article 5 for the first time. The terrorist attacks in Paris on 13 November 2015, which led France to invoke Article 42(7), were also executed by non-state actors [54].

Cyberattacks, making use of the virtual dimension, might prove to be even more challenging to align with the system of collective defence [55]. Not only are non-state actors active in cyberspace, but moreover, cyberattacks predominantly fall below the threshold of the use of force. Two questions must therefore be addressed: can cyberattacks amount to the level of an armed attack, and if not, the subsequent question is whether the collective defence system is applicable to attacks below the threshold of the use of force?'

Armed attacks comprise (i) transnational (ii) use of force, which will have a (iii) substantial impact [56] in terms of (iv) scale and effect [57]. Cyberattacks could amount to the level of an armed attack, if they cause effects 'resulting in physical casualties, substantial physical damage, or such substantial and long-term damage to critical infrastructure that the carrying out of a state's essential functions or its social and political stability are seriously impaired' [58].

Recent cyberattacks have not amounted to the level of use of force (with the possible exception of the 2010 Stuxnet attack) [59], let alone of an armed attack. However, as cyber operations are capable of inflicting crippling effects [60], it is not unlikely that a cyberattack might indeed reach this magnitude [61], and potentially lead to the invocation of current collective defence systems.

Until such a conjuncture, the subsequent question would therefore be if the NATO and EU collective defence systems, including the EU solidarity clause, should, based on state practice and legal opinion, be reinterpreted taking into account the attributes of cyberattacks. Cyber operations are often executed by (elusive) non-state actors, the activities predominantly falling below the theshold of an armed attack, and even below the use of force.

(53) Lanovoy, V., 'The use of force by non-state actors and the limits of attribution of conduct', *European Journal of International Law*, Vol. 28, May 2017, pp. 567-568, p. 563.

(54) 'Article 42.7: An Explainer', op. cit.

(55) See 'Implementing Article 42.7 of the Treaty on European Union', op.cit., pp. 14-15.

(56) Gill, T.D. and Tibori-Szabó, K., 'Twelve key questions on self-defense against non-state actors – and some answers', ACIL, *International Legal Studies*, Vol. 95, 2019, p. 492.

(57) Boothby, W.H. et al, 'When is a cyberattack a use of force or an armed attack?', *Computer*, Vol. 45, 2012, p. 82; *Case concerning military and paramilitary activities in and against Nicaragua,* op. cit., Para 195; 'Implementing Article 42.7 of the Treaty on European Union', op.cit., p. 9; Ducheine, P. A.L., 'Military cyber operations' in Gill, T.D. and Fleck, D. (eds), *The Handbook of the International Law of Military Operations*, 2nd edition, Oxford University Press, Oxford, 2015, pp. 456-475.

(58) 'Anticipatory self-defense in the cyber context', pp. 460-461.

(59) An eloquent analysis can be found in: Efrony, D. and Shany, Y.,'A rule book on the shelf? Tallinn Manual 2.0 on cyber operations and subsequent state practice', *American Journal of International Law*, Vol. 112, No 4, 2018, pp. 594-631. On Stuxnet see: Schmitt, M.N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017, Rule 71(10), p. 342; Sanger, D.E., *The Perfect Weapon : War, sabotage, and fear in the cyber age*, Scribe, 2018 (chapter 1).

(60) Referring to recent cyber-attacks and incidents, including SolarWinds, Colonial Pipeline systems and the US executive order in response to that, see: The White House, 'Executive Order on Improving the Nation's Cybersecurity', May 2021 (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/).

(61) For an earlier – more reserved – assessment, see 'Anticipatory self-defense in the cyber context', op.cit., p. 461.

The issue of non-state actors is less problematic. Although Article 51 of the UN Charter (and therefore the derivative Article 5 of the NATO Treaty and Article 42(7) TEU) has been incorporated in treaties regulating state behaviour, this does not impair the inherent or customary international rule of self-defence, also against non-state actors [(62)]. After 9/11, this now also appears to be a common interpretation of Article 51 UN Charter itself [(63)].

The fact that the customary international right of self-defence also applies to armed attacks by non-state actors does not, however, solve the collective cyber defence conundrum. The difficulty lies in the combination of a non-state cyberattack below the threshold of an armed attack, that cannot be attributed to a specific perpetrator, or (territorially) located.

The customary international right to self-defence and hence Article 51 UN Charter, Article 5 NATO Treaty and Article 42(7) TEU, establish the legal basis for responding to armed attacks. The remit could be widened to include 'armed aggression' or even the use of force [(64)]. The United States have, after the *Nicaragua* Case [(65)], refrained from distinguishing between the use of force and an armed attack [(66)], hence, in their view, any form of the use of force can invoke the right of self-defence. However, this legal opinion is not universally held. Using 'armed aggression' instead of 'armed attack' could, liberally reading into the intention of the EU drafters, also stretch the remit of collective defence to include responses to use of force. However, both interpretations will not suffice since a cyberattack could not only fall below the level of armed attack but also below the level of the use of force. Furthermore, from a legal point of view, stretching this standard would be untenable since an armed attack invokes the inherent right of self-defence, while (other) use of force in an interstate setting does not, although the execution of a cyberattack may authorise such responses as countermeasures [(67)] excluding the use of force [(68)]. However, countermeasures are inherently unilateral in the sense that only the injured state (or states) can appeal to them [(69)]; collective countermeasures are not allowed [(70)].

The solidarity clause (Article 222 TFEU) could be used in response to a broader array of attacks, including those below the use of force. Although the solidarity clause is confined to terrorist attacks and natural or man-made disasters, the meaning of disaster is rather broad and includes 'any situation which has or may have a severe impact on people (…)' [(71)]. The 2013 EU Cybersecurity Strategy also alluded to the possibility of invoking Article 222 TFEU in case of a serious cyberattack [(72)].

---

(62) 'Twelve key questions on self-defense against non-state actors – and some answers', op.cit., p. 474.

(63) Ducheine, P.A.L. and Pijpers, P. BMJ., 'The missing component in deterrence theory: The legal framework', ACIL Research Paper 2020-70, 2020., pp. 494-495; 'Implementing Article 42.7 of the Treaty on European Union', op.cit., p. 6.

(64) 'Mutual Assistance Clauses of the North Atlantic and EU Treaties', op.cit., pp. 422-425.

(65) *Case Concerning Military and Paramilitary Activities in and against Nicaragua*, op.cit..

(66) Hongju Koh, H., 'International Law in cyberspace', 4854 Faculty Scholarship Series 1, 2012, p. 7; Schmitt, M.N., 'The Defense Department's measured take on International Law in cyberspace', *Just Security,* 11 March 2020 [Section on 'The use of force'] (https://www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/).

(67) 'The missing component in deterrence theory', op.cit., p. 491.

(68) Article 50 (1) a of the United Nations, 'Responsibility of states for internationally wrongful acts', 2001, II *Yearbook of the International Law Commission* vol II (Part Two).

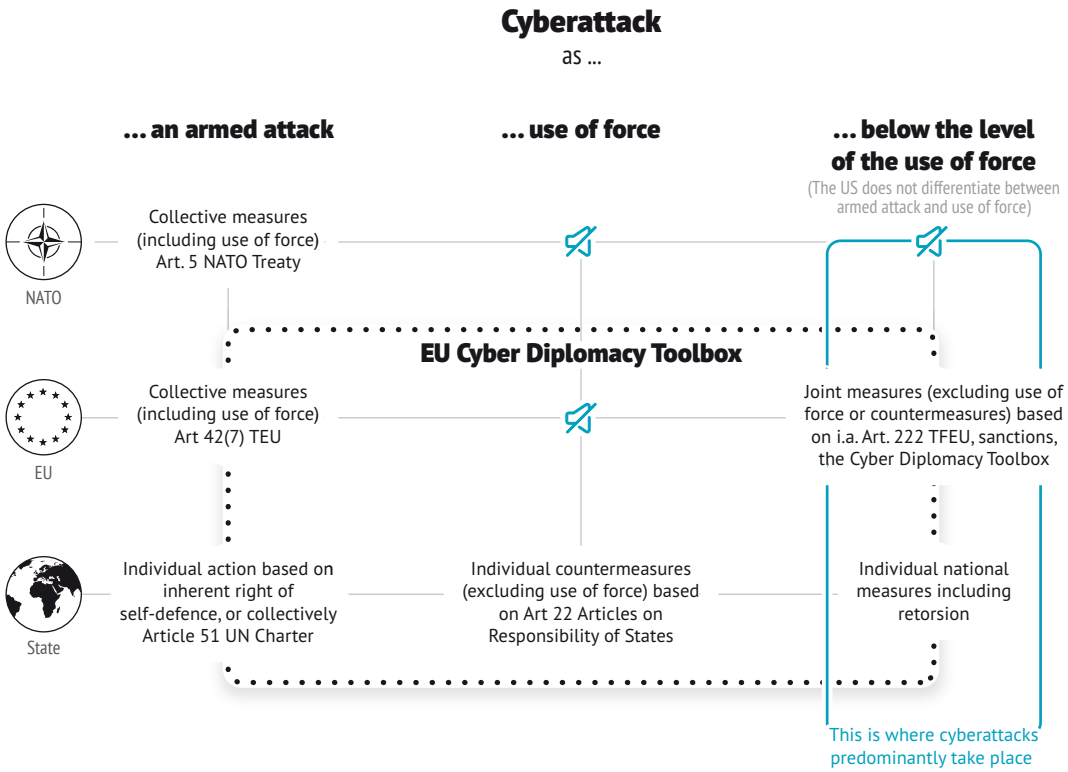
(69) Roguski, P., 'Collective countermeasures in cyberspace – Lex lata, progressive development or a bad idea?', International Conference on Cyber Conflict, CYCON 25, 26-29 May 2020, pp. 27-31.

(70) Delerue, F., *Cyber Operations and International Law*, Cambridge University Press, Cambridge, 2020, p. 232.

(71) Council of the European Union, 'Decision on the arrangements for the implementation by the Union of the solidarity clause', op.cit., Article 3 (a), p, 55; 'Cybersecurity and cyberdefence: EU solidarity and mutual defence clauses', op.cit., p. 4.

(72) European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace', (Join(2013) 1 final), February 2013, p. 19 (https://edps.europa.eu/sites/default/files/publication/13-02-07_communication_join_cyber_sec_en.pdf).

Collective cyber defence and the EU Cyber Diplomacy Toolbox



The EU solidarity clause widens the options to other, more generic collective cybersecurity options than the inherent right of self-defence, individually or collectively, and thus not in response to an armed attack or the use of force. While NATO is able to issue statements regarding unwelcome situations in its territorial perimeter [(73)], it basically lacks instruments of power in the remit below the use of force. This should not be surprising, since this is not NATO's purpose. The opposite applies to the EU. Although the EU has some arrangements regarding responses to an armed attack, the core of its instruments – consistent with the identity of the EU as a soft power – are not related to the use of force. The EU has numerous tools within these instruments of power ranging from restrictive measures (sanctions) [(74)] to recalling diplomats and issuing demarches. In legal terms the responsive measure amounts to retorsions: unfriendly albeit lawful activities [(75)]. It is also in this area (see diagram above) that most cyberattacks take place. To address malign activities in cyberspace, the EU has a joint response mechanism in which Union and Member States' tools

(73) For example: NATO, 'North Atlantic Council Statement following the announcement by the United States of actions with regard to Russia', 15 April 2021 (https://www.nato.int/cps/en/natohq/news_183168.htm#:~:text=Issued%20on%20 15%20April%202021&text=NATO%20Allies%20support%20and%20stand,enhance%20the%20Alliance's%20collective%20 security.)

(74) Title IV, Article 215 on Restrictive Measures, 'Treaty on the Functioning of the European Union', *OJ* C 326, 26 October 2012 (https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:326:FULL:EN:PDF)..

(75) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*., op.cit., Rule 20 (4).

are collected in the so-called cyber diplomacy toolbox [(76)]. Although this toolbox is not a coherent foreign policy instrument but rather a potpourri of options, it demonstrates the potency of a collective cyber defence mechanism against cyberattacks below the use of force [(77)].

REFLECTIONS ON THE ROLE OF THE EU

Is the EU better equipped to provide a collective defence system against cyberattacks than NATO?

It can be assessed that, firstly, cyberattacks predominantly fall below the threshold of the use of force, which implies that collective defence clauses designed for armed attacks are incompatible with most cyberattacks. Secondly, cyberattacks are often executed by non-state actors. Although Article 51 UN Charter was meant to regulate state behaviour, the inherent right of self-defence it reflects is a separate rule of customary international law [(78)]. The latter includes attacks by non-state actors, and after the 9/11 attack Article 51 UN Charter is also commonly interpreted in that sense. Thirdly, the author and the origin of cyberattacks (state or non-state actors) are sometimes difficult to pinpoint, given the time-lapse between the malign cyber-activity and the actual effect of a cyber-attack. Establishing authorship and attributing a cyberattack to an actor or even a state, without conclusive technical and forensic evidence is possible but is a political act. Nevertheless, and although with lower (overt) standards of certainty, attribution is on the rise. Fourthly, since cyberattacks target the cognitive dimension via cyberspace, these attacks seldom have a physical or functional manifestation, making it challenging to conclude that the territory of an EU or NATO Member State is affected.

The EU, as an integrated and political entity, has a broader scope than NATO which can be used to tackle many issues related to cyberattacks. The EU competences coalesce with the attributes of current cyberattacks, especially when related to problems of attribution, the virtual characteristics of the cyberattack, but primarily given the fact that cyberattacks remain below the threshold of the use of force.

In that sense, the EU is better suited to respond to cyberattacks. The EU is able to focus on collective measures below the use of force including diplomatic, economic and other instruments, thereby complementing NATO and not latently competing with it. However, while the current cyber diplomacy toolbox is a welcome first step, it is insufficient as a coherent EU joint response mechanism as it lacks focus. To strengthen EU policy related to a joint response to cyberattacks, the EU response mechanism would need to operate separately from collective responses to armed attacks since the latter are based on the inherent right of self-defence of Member States – individually or collectively. It should also operate autonomously from responses by individual Member States, which include countermeasures against the use of force. Since collective countermeasures by the EU are not allowed, the EU's joint response mechanism against cyberattacks should revolve around lawful but unfriendly retorsions, including collective EU sanctions and issuance of diplomatic statements attributing cyberattacks to alleged perpetrators.

(76) European Union, 'Joint EU diplomatic response to malicious cyber activities ("Cyber Diplomacy Toolbox")', Draft Council Conclusions, 2017; Moret, E. and Pawlak, P., 'The EU Cyber Diplomacy Toolbox: Towards a cyber sanctions regime?', Brief no. 24, European Union Institute for Security Studies, July 2017.

(77) Ivan, P., 'Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox', European Policy Centre, March 2019, pp. 11–12.

(78) 'When is a cyberattack a use of force or an armed attack?', op.cit., p. 83.