DOI 10.5817/MUJL2022-1-4

EU COMMON POSITION ON INTERNATIONAL LAW AND CYBERSPACE[1]

by

ANNA-MARIA OSULA, AGNES KASPER, ALEKSI KAJANDER[*]

The discussion on international law applicable to cyber operations has shifted from asking whether international law applies to cyberspace to how it applies. Recently the European Union declared in its renewed cybersecurity strategy the ambition to develop common EU position on the application of international law in cyberspace. As part of a broader vision in striving for leadership on standards, norms and regulatory frameworks in cyberspace, the joint communication underlined the need for taking a more proactive stance in the discussions at the United Nations and other relevant international fora. However, less than half of the European Union Member States have issued a public statement on the interpretation of international law in cyberspace and hence, reaching a consensus on the interpretation of relevant concepts of international law appears a challenge. This article provides an overview of the current status of European Union Member States' public statements on international law applicable to cyber operations, identifies the domains of international law where convergence of views can be observed and highlights the areas with notable differences.

[1] Anna-Maria Osula's research for this article was supported by the Masaryk University ERDF project "Cyber Security, Cyber Crime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01 / 0.0 / 0.0 / 16_019 / 0000822). The contribution by Agnes Kasper is part of the cooperation within Jean Monnet Network "European Union and the Challenges of Modern Society" (611293-EPP-1-2019-1-CZ-EPPJMO-NETWORK). The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects only the views of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

[*] anna-maria.osula@taltech.ee; Senior researcher at Tallinn University of Technology, Estonia; Research fellow at Masaryk University, Czech Republic.
agnes.kasper@taltech.ee; Senior lecturer at Tallinn University of Technology, Estonia.
aleksi.kajander@taltech.ee; Early stage researcher at Tallinn University of Technology, Estonia.

KEY WORDS

European Union, International law, Cyber norms, Cyber security, United Nations, Cyberspace, Cyber law

1. INTRODUCTION

International law, norms, confidence- and capacity-building form the backbone for current discussions aiming at building and maintaining trust and security in the digital environment. International law forms the foundation for stability and predictability between states as it reflects common views of accepted state behaviour. International law also offers options for legal responses to cyber operations targeted against a state. In particular, adherence to international law plays an important role in protecting small nations who lack military power or resources.[2] Arguably, the predictability provided by international law may potentially act as deterrence against possible malicious cyber operations.

By now, the discussion on international law has shifted from asking *whether* international law applies to cyberspace to *how* it applies.[3] With some exceptions (such as the Council of Europe Budapest Convention on Cybercrime), there are no international agreements currently tailored specifically for regulating state behaviour in cyberspace. Therefore, state practice and national declarations on how states interpret international law applicable to cyber operations are valuable for increased legal certainty and transparency. However, currently only a fairly limited number of states have published comprehensive views on international law in cyberspace.[4]

With individual countries hesitating to publish national views, regional and international organisations have the potential to facilitate discussions and provide platforms for reaching a consensus. So far, few international organisations have successfully reached a consensus among their members on aspects of international law and cyberspace (such as the UN and NATO which will be discussed below). Many others have simply expressed their general support on the applicability of international law in cyberspace.[5]

However, recently the European Union (EU) declared in its renewed cybersecurity strategy the ambition to develop a common EU position

---

[2] Osula, A. (2021) *'Aligning Estonian and Japanese Efforts in Building Norms in Cyberspace', So Far, Yet So Close: Japanese and Estonian Cybersecurity Policy Perspectives and Cooperation*. Tallinn: International Centre for Defence and Security, p. 23.

on the application of international law in cyberspace. As part of a broader vision of striving for leadership on standards, norms and regulatory frameworks in cyberspace, the joint communication underlined the need for taking a more proactive stance in the discussions at the UN and other relevant international fora. Moreover, it emphasized that the EU is best placed to "*advance, coordinate and consolidate Member States' positions in international fora*".[6]

Against this backdrop the aim of the article is to give an overview of the current status of EU MSs' public statements on international law applicable to cyber operations, identify the domains of international law where convergence of views can be observed and highlight the areas with

[3] EU has an unwavering position regarding the applicability of international law in cyberspace. Equally, the applicability of human rights in cyberspace is uncontroversial among the EU MSs and there is consensus that human rights law applies online the same as it does offline. See E.g. Ministry for Foreign Affairs and International Cooperation (2021) *Italian Position Paper on 'International Law and Cyberspace'.* Rome: Ministry for Foreign Affairs and International Cooperation. Available from: https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf [Accessed 7 January 2022],p. 10. Austria (2020). *Pre-draft Report of the OEWG – ICT Comments by Austria.* Available from: https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf [Accessed 14 January 2022], pp. 3-4. United Nations General Assembly (2021) *Official compendium of voluntary national contributions on the subject of how international technologies by States submitted by participating government experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established pursuant to General Assembly resolution 73/266.* New York: United Nations General Assembly. Available from: https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf [Accessed 14 January 2022], p. 78. Government of the Kingdom of Netherlands (2019) *Appendix: International law in cyberspace*. Available from: https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf [Accessed 7 January 2022, p. 5, Slovenia (2021) *Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, Informal virtual meeting (18, 19 and 22 February 2021) Slovenia Statement*. Available from: https://front.un-arm.org/wp-content/uploads/2021/02/Slovenia-19-February-2021-FINAL.pdf [Accessed 14 January 2022], p. 2., Ministry of Foreign Affairs of Finland (2020) *International law and cyberspace Finland's national positions.* [online] Available from: https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727 [Accessed 7 January 2022], pp. 7-8, Estonia (2021) *Estonian contribution on the subject of how international law applies to the use of information and communications technologies by states, to be annexed to the report of the Group of Governmental Experts on Advancing responsible state behaviour in cyberspace (2019-21).* Available from: https://ccdcoe.org/uploads/2018/10/Estonian_contribution_on_international_law_to_the_gge_may_2021_English.pdf [Accessed 14 January 2022], p. 5. See also NATO (2020) *Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace Operations*. Brussels: NATO Standardization Office, 19.

[4] From the EU countries, citing the most recent ones; Austria (2020) op. cit., Estonia (2021) op. cit, Government of the Kingdom of Netherlands (2019) op. cit., Czech Republic (2020) op. cit., Italy: Ministry for Foreign Affairs and International Cooperation (2021) op. cit., Romania: United Nations General Assembly (2021A) op. cit., pp. 75-79, Germany: The Federal Government (2021) op. cit., France: Ministere Des Armees (2019) op. cit., Finland: Ministry of Foreign Affairs of Finland (2020) op. cit.

notable differences. As such the article seeks to provide useful analysis for the future endeavours of the EU in fulfilling the objective set in 2020.

2. INTERNATIONAL DISCUSSIONS ON INTERNATIONAL LAW

Before analysing individual EU MS's interpretation of international law applicable to cyber operations, it is relevant to review the extent of a common position formed on other international fora, namely the UN and NATO, as this can offer a useful starting point for identifying pan-EU communalities. Such analysis also points out the areas where the interpretations of EU MSs rest upon the consensus reached on international fora, and where they have been further elaborated upon.

The UN is the most active platform for discussing norms for states in cyberspace. Since 1998, when the Russian Federation first introduced a draft resolution on information security in the First Committee of the UN General Assembly,[7] the UN Secretary-General has been issuing annual reports with the views of UN MSs to the General Assembly (GA).[8] Groups of Governmental Experts (GGEs) have been formed in 2004/5, 2009/10, 2012/13, 2014/15, 2016/17 and 2020/21 with the total of four consensus reports (in 2010, 2013, 2015, 2021) to examine the existing and potential threats from the cyberspace and possible cooperative measures to address them.[9] Notably, the 2015 UN GGE report was adopted also as the GA

[5] E.g. Organization of American States (2021) *AG/RES. 2959 (L-O/20) International Law.* Washington: Organization of American States. Available from: http://www.oas.org/en/sla/iajc/docs/AG-RES_2959_EN.pdf [Accessed 14 January 2022]; Association of Southeast Asian Nations (2018) *ASEAN Leaders' Statement on Cybersecurity Cooperation*, Singapore: Association of Southeast Asian Nations. Available from: http://setnas-asean.id/site/uploads/document/document/5b04cdc25d192-asean-leaders-statement-on-cybersecurity-cooperation.pdf [Accessed 14 January 2021] and G20 (2015) *G20 Leaders' Communiqué Antalya Summit, 15-16 November 2015*. Anatalaya:G20, Available from: https://www.gpfi.org/sites/gpfi/files/documents/G20-Antalya-Leaders-Summit-Communiqu--.pdf [Accessed 14 January 2022].

[6] European Commission (2020) *Joint Communication to the European Parliament and the Council the EU's Cybersecurity Strategy for the Digital Decade*. Brussels: European Commission. Available from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 [Accessed 20 January 2022], p. 20.

[7] United Nations General Assembly (1999) *Resolution Adopted by the General Assembly [on the report of the First Committee (A/53/576).* New York: United Nations General Assembly. Available from: https://undocs.org/en/A/RES/53/70 [Accessed 14 January 2022].

[8] United Nations Office for Disarmament Affairs. *Developments in the field of information and telecommunications in the context of international security.* New York: United Nations Office for Disarmament Affairs. Available from: https://www.un.org/disarmament/ict-security/ [Accessed 14 January 2022].

resolution 70/237, calling all MSs to „*be guided in their use of information and communications technologies by the 2015 report of the [GGE].*"[10]

Although the 2010 UN GGE consensus report did not directly address international law, the following GGE reports have established the essential role of international law in reducing risks to international peace, security and stability. In 2013 the GGE consensus report put forward the landmark position that "*international law and in particular the [UN] Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment*" and included a set of recommendations on norms, rules and principles of responsible behaviour by states.[11] The 2015 GGE report featured a specific section on how international law applies to the use of ICTs and mentioned several international law concepts relevant to state behaviour in cyberspace.[12] The 2021 GGE report expanded the consensus even further by, *inter alia*, underlining the applicability of international humanitarian law in cyberspace and pleading countries not to conduct and support cyber operations targeting critical infrastructure, including the technical infrastructure essential for the Internet and health sector entities. Over the years, the UN GGE has invited its participating governmental experts to provide voluntary national contributions about how international law applies to the use of ICTs by states.[13]

---

[9] The UN GGE convened in 2009 and 2016 did not reached consensus report. However, reports were published in 2010 (A/65/201), 2013 (A/68/98*) and 2015 (A/70/174). United Nations Office for Disarmament Affairs (2019) *Fact Sheet Developments in the field of information and telecommunications in the context of international security*. New York: United Nations Office for Disarmament Affairs. Available from: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf [Accessed 14 January 2022].

[10] United Nations General Assembly (2015A) *Resolution adopted by the General Assembly on 23 December 2015 [on the report of the First Committee (A/70/455) 70/237*. New York: United Nations General Assembly. Available from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/457/57/PDF/N1545757.pdf?OpenElement [Accessed 14 January 2022].

[11] United Nations General Assembly (2013) *Resolution adopted by the General Assembly on 23 December 2015 [without reference to a Main Committee (A/68/L.26 and Add. 1)] 68/98*. New York: United Nations General Assembly. Available from: https://undocs.org/A/RES/68/98 [Accessed 14 January 2022].

[12] United Nations General Assembly (2015B) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: United Nations General Assembly. Available from: https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 [Accessed 14 January 2021].

[13] E.g. the 2021 report included the opinions of 15 countries in United Nations General Assembly (2021A) op. cit.

In addition to the GGE process, the UN Open-Ended Working Group (OEWG) also concluded a consensus report in 2021.[14] The report set a precedent by reflecting the discussions held among all UN MSs and *inter alia* focused on how international law applies to the use of ICTs by states. The final text offered broad support to the framework for responsible state behaviour, the general applicability of international law as well as norms developed by the previous efforts of the UN GGE, notably the GGE 2015 report.

As an important development, the North Atlantic Treaty Organisation NATO has published in 2020 an *Allied Joint Doctrine for Cyberspace Operations* (hereafter AJP-3.20) which reflects the (almost) consensus of 30 NATO members. The document is intended primarily as guidance for NATO commanders, staffs and forces while also providing guidance for NATO Members, partners, non-NATO nations and other organisations. The document clearly states that the adopted framework sets out the parameters within which its military forces can operate and that international law provides prescriptions and limitations for both forces and individuals.[15]

While it is important to note that the reports adopted by the UN GGE and OEWG are not law-making processes *per se*, they still have a significant role to play in pinpointing legal concepts supported and valued internationally, and thereby shaping and establishing international agreement on accepted state behaviour in cyberspace. Equally, the AJP-3.20 does not only reflect an agreement among a military organisation, but also indicates a common view of 21 EU MSs which is an indication of larger convergence of views among EU MSs than what can be deduced from analysing individual domestic positions.

---

[14] United Nations General Assembly (2021B) *Open-ended working group on developments in the field of information and telecommunications in the context of international security*. New York: United Nations General Assembly. Available from: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf [Accessed 14 January 2022].

[15] NATO (2020) op. cit., pp. xiii, 20, 22. See also Schmitt, M. (2020) *Noteworthy Releases of International Cyber Law Positions – Part I: NATO*, New York: Lieber Institute West Point. Available from: https://lieber.westpoint.edu/nato-release-international-cyber-law-positions-part-i/ [Accessed 14 January 2022].

3. COMMON THEMES IN THE EU MEMBER STATES' OFFICIAL VIEWS

Our research has identified public statements pertaining to the interpretation of international law and cyber operations, or mentioning related concepts, from the majority of EU MSs. However, in most of these cases, the identified documents were broadly worded and did not go into detail with legal discussions. Nevertheless, we determined nine EU MSs' declarations, all referenced to in this article, to be more extensive and thereby useful in shedding light to the scope of the EU MSs' common and diverging views. It must be underlined that the national positions we have analysed are in many aspects much more nuanced then referenced below, while at the same time it has been challenging to assess the meaning of some aspects which have (deliberately or not) not been mentioned in the positions.

In addition to national positions, we have also considered the UN GGE and OEWG reports, related EU documents and the AJP-3.20 publication. Given that the UN GGE 2015 report has been endorsed by the UN GA, we view this document as reflecting the broad consensus of UN MSs. The OEWG report and AJP-3.20 reflect respectively the consensus of the UN and NATO members.

3.1 SOVEREIGNTY

Sovereignty is no doubt one of the most politically loaded terms in the discussions revolving around state behaviour in cyberspace. The relevance of the concept of sovereignty in cyberspace has been endorsed in the UN GGE and OEWG reports and mentioned by all nine EU MSs who have published their more detailed legal views.

In the debate on whether sovereignty should be considered as principle[16] of international law or a principle *and a* standalone rule, the breach of which would entail an internationally wrongful act, the EU MSs' approach appears rather unified. AJP-3.20 includes a reference to sovereignty as a rule,[17] thereby reflecting the common position of twenty one EU MSs

[16] For the UK position see: Wright, J. (2018) *Cyber and International Law in the 21st Century*. London: Chatham House. Available from: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [Accessed 14 January 2022]

[17] NATO (2020) op. cit., p. 20, footnote 26.

who also belong to NATO, making the total number of EU MSs having expressed support for sovereignty as a rule twenty three.

For example, and in the aftermath of the foiled cyberattack targeting the OPCW, the Netherlands was one of the firsts in September 2019 to state publicly that "*respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act*".[18] About the same time, France also issued an elaborate document detailing its interpretations of the international law applicable to cyber operations and made clear that it may consider certain cyberattacks against French digital systems or any effects produced on French territory by digital means a breach of sovereignty as long as state attribution can be established – hence violation of sovereignty as a rule is conceivable.[19] Estonia[20], Austria[21], Finland[22], Czech Republic[23], Germany[24], Romania[25] and Italy[26] followed in suit, all agreeing that sovereignty entails both rights and obligations, and essentially, that violation of sovereignty by a cyber operation is capable of being an internationally wrongful act. These positions are summarised below in Chart 1.

---

[18] Government of the Kingdom of Netherlands (2019) op. cit., p. 2.

[19] Ministere Des Armees (2019) *International Law Applied To Operations in Cyberspace*. Paris: Delegation a l'information et a la communication de la defense. Available from: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf [Accessed 7 January 2022].

[20] ERR News (2019) *President Kaljulaid at CyCon 2019: Cyber attacks should not be easy* weapon. Tallinn: ERR News. Available from: https://news.err.ee/946827/president-kaljulaid-at-cycon-2019-cyber-attacks-should-not-be-easy-weapon [Accessed 14 January 2022]. Also in United Nations General Assembly (2021) op. cit., p. 26.

[21] Austria.(2020) op. cit., p. 3.

[22] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 7.

[23] Czech Republic (2020) *Czech Republic Statement by Mr. Richard Kadlcak Special Envoy for Cyberspace Director Cyberseuciryt Department at the 2nd substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations*. New York: United Nations General Assembly. Available from: https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf [Accessed 14 January 2022], p. 3.

[24] The Federal Government (2021) *On the Application of International Law in Cyberspace*. Berlin: German Federal Foreign Office. Available from: https://ccdcoe.org/uploads/2018/10/Germany_on-the-application-of-international-law-in-cyberspace-data_English.pdf [Accessed 7 January 2022], p. 3.

[25] United Nations General Assembly (2021A) op.cit., p. 76.

[26] Ministry for Foreign Affairs and International Cooperation (2021) op.cit., p. 4.

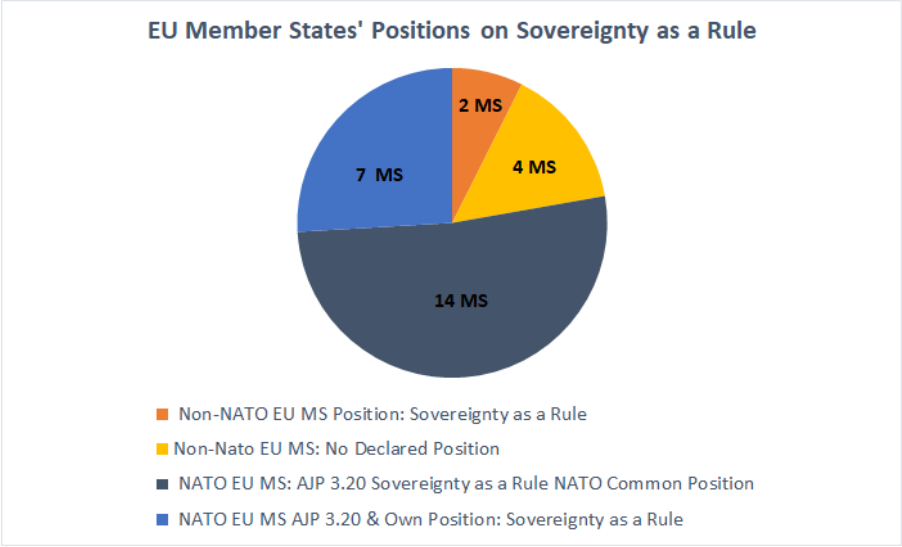

Chart 1.

Based on the EU MSs' positions, the most supported approach is that sovereignty is a principle and rule, entailing both rights and obligations. Its components are internal and external sovereignty, and they also apply in cyberspace. The authority of the state to exercise sovereignty is not unlimited. Cyber operation attributable to a state that causes non-negligible harmful tangible impact on the territory of the target state will likely violate territorial sovereignty.

All EU MSs' positions distinguish between internal and external aspects of sovereignty, but some chose to emphasize or simply limit its position to a specific aspect in their general discussion of sovereignty. The German and Czech positions remain closely linked to territory and effects caused therein, and the Netherlands elaborates in detail on internal sovereignty. Taking a somewhat different route, Romania focuses on immaterial dimensions, Finland brings specific examples illustrating that a "*state possesses a legal interest in the protection of its territory from any form of external harmful action*".[27] France[28], Finland[29] and Estonia[30] use wordings that leave the door open to consider cyber operations where the targeted infrastructure is located outside their territory (e.g. in case of use of cloud

[27] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 2 referring to Nuclear Tests (Australia v. France), Judgment, I.C.J. Reports 1974, p. 253, para. 456.

[28] Ministere Des Armees (2019) op. cit., p. 7.

[29] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 2.

[30] United Nations General Assembly (2021A) op. cit., p. 24.

services). A particularly clear position is formulated by France, whereas France "*exercises jurisdiction over information systems located in its territory*" and adds in a footnote that also over "*connected objects /.../ and content operated or processed via electronic communication networks which cover the national territory or from an IP address attributed to France*"[31].

What constitutes a violation depends on the characteristics of the operation in question, and case-by-case assessment is needed. Estonia briefly notes that "*[v]iews on what constitutes a breach of sovereignty in cyberspace differ. Malicious cyber operations can be complex, cross several jurisdictions and may not always produce physical effects on targeted infrastructure*"[32], leaving the discussion of the threshold for a later opportunity. Romanian and Italian positions are also non-specific, the former reaffirming that interference with or preventing the state from exercising its sovereign prerogatives can be considered breach of sovereignty[33], the latter "*considers that the principle in question prohibits a [s]tate from conducting cyber operations, which produce harmful effects on the territory of another [s]tate, irrespective of the physical location of the perpetrator*"[34].

Some states go further. For the Netherlands, the nature and consequences entail "*1) infringement upon the target [s]tate's territorial integrity; and 2) there has been an interference with or usurpation of inherently governmental functions of another [s]tate*", concurring with the Tallinn Manual in this respect.[35] Germany hints that interference with the political independence of a state, absent coercion, may in certain circumstances also constitute a breach of sovereignty, but it sets a de minimis limit to necessary *physical effects and functional impairments* that can be deemed to constitute violation of *territorial* sovereignty[36]. Czech Republic[37] and Finland too make it clear that in addition to material harm as a qualifier for breach of territorial sovereignty, loss of functionality can also be a base for claiming violation of sovereignty. In addition, Finland holds that relevant considerations include operations with the effect below the threshold of loss

[31] Ministere Des Armees (2019) op. cit., p. 6.
[32] United Nations General Assembly (2021A) op. cit., p. 25.
[33] United Nations General Assembly (2021A) op. cit., p. 76.
[34] Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 4.
[35] Government of the Kingdom of Netherlands (2019) op. cit., p. 3.
[36] The Federal Government (2021) op. cit., p. 4.
[37] Czech Republic (2020) op. cit., p. 3.

of functionality, i.e. modification or deletion of information belonging to the target state, or to private actors in its territory.[38]

Finally, France first defines the term cyberattack[39], then it considers that any such cyberattack attributable to a state, against French digital systems or effects produced on French territory by digital means constitutes at least breach of sovereignty[40]. It appears that for France, even a failed cyberattack that does not cause any actual harm or effect, could still constitute breach of sovereignty, since the criteria set has two main elements: the operation 1) qualifies as a cyberattack under the definition; and 2) is attributable to a state. One should note here that cyber operations *intended to* cause damage or which *may* cause harm[41] also fall under the definition. The French position seems to set the lowest threshold, from the ones under scrutiny here, and the nature of the operation is the major determinant for considering what constitutes violation of sovereignty.

3.2 DUE DILIGENCE

Due diligence has been touched upon in the GGE 2015 consensus report in two occasions. Firstly, as a principle according to para. 13 (c) states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. Secondly, but in a much narrower formulation, the principle is also recognizable in the section addressing international law, in para. 28 (e) under which states must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to commit such acts.[42]

Nine EU MSs' positions considered due diligence, hence it is a key issue, closely linked to the principle of sovereignty and state responsibility, however the modalities of application in cyberspace are less than straightforward.

Netherlands, Germany, Italy, Romania and Finland refer to the ICJ's Corfu Channel judgment, confirming the binding nature of the due diligence rule. However, France and Estonia point to the 2015 GGE report

[38] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 2.

[39] Ministere Des Armees (2019) op. cit., p. 6. footnote 7. Cyberattack is "deliberate, offensive and malicious action taken via cyberspace that is intended to cause damage (in terms of availability, integrity or confidentiality) to information or the systems that process it and that may harm the activities of which it or they are the medium".

[40] Ministere Des Armees (2019) op. cit., p. 7.

[41] Ministere Des Armees (2019) op. cit., p. 6, footnote 7.

[42] United Nations General Assembly (2021A) op. cit.

para. 13 (c), where due diligence *principle* in a non-binding format is set out, which countries *should* follow; nevertheless, these states also use a language that indicates the binding nature of the due diligence. France posits that it is a customary obligation[43], while Estonia uses the wording that "*states have to make reasonable efforts to ensure that their territory is not used to adversely affect the rights of other states*". [44] Austria literally underlines that "*[s]tates must seek to ensure that their territory is not misused for the commission of internationally wrongful acts using ICTs*".[45]

Majority of positions[46] point out or imply by their language that it is an obligation of conduct, not result, and that "*knowledge*"[47] is a constitutive element of the obligation to arise. However, a few remain silent on both matters, therefore conclusions can be drawn only with these limitations. Compliance with this obligation is by taking feasible or reasonable measures when another state suffers consequences of certain gravity. While numerous states hint that feasibility, or what can be considered reasonable, is a variable standard[48], contextual[49] and can depend on the various capabilities of the state in question[50], no common position can currently be deducted from those. The precise cyber threshold for triggering the due diligence obligation also remains unclear, but there seems to be a tendency to argue that the consequences need to be sufficiently adverse, but not necessarily in the form of physical damage.[51] Yet only few refer to a positive obligation to protect human rights explicitly as a trigger for due diligence obligation.[52]

Generally, the aim of such due diligence measures is to prevent or halt harmful activities, their consequences on the target state or activities which

---

43 Ministere Des Armees (2019) op. cit., p. 6.

44 United Nations General Assembly (2021A) op. cit., p. 26. Emphasis added.

45 Austria (2021) *Comments by Austria on the Zero-Draft for the OWEG's Final Report*. Available from: https://front.un-arm.org/wp-content/uploads/2021/02/Austria-Comments-Zero-Draft-OEWG-19.02.2021.pdf [Accessed 14 January 2022].

46 Estonia (2021) op. cit., Government of the Kingdom of Netherlands (2019) op. cit., Ministry for Foreign Affairs and International Cooperation (2021) op. cit., United Nations General Assembly (2021) op. cit.

47 Ibid.

48 Ministry of Foreign Affairs of Finland (2020) op. cit., p. 4.

49 Government of the Kingdom of Netherlands (2019) op. cit., p. 5.

50 Estonia (2021) op. cit., p. 26, Government of the Kingdom of Netherlands (2019) op. cit.

51 Government of the Kingdom of Netherlands (2019) op. cit., p. 5.

52 Ministry of Foreign Affairs of Finland (2020) op. cit., p. 5; Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 6.

carry the risk of causing significant transboundary harm.[53] However, the term "*prevention*" in this context usually refers to an obligation relating to ongoing or imminent operations, and essentially means to stop them or their consequences.[54] Estonia offered a more progressive view on this point, linking the due diligence principle with capacity building, and proposing that "*[s]tates should strive to develop means to offer support, when requested by the injured state, to identify or attribute malicious cyber operations*"[55].

Finally, while other states also mention potential violations of due diligence obligation, France pays more attention to this question, expressing that a "*state's failure to comply with this obligation is not a ground for an exception to the prohibition of the use of force*".[56]

3.3 INTERVENTION

Whereas the UN GGE 2021[57] and 2015[58] reports mention the principle of non-intervention, it is not included in the OEWG report nor in AJP-3.20. Based on our research seven EU MSs have publicly shared their views on prohibited intervention.

It is generally agreed that the obligation of non-intervention prohibits states from intervening coercively in the internal or external affairs of other states. Even though the obligation of non-intervention is not explicitly mentioned in the UN Charter, it can be derived as a corollary of the sovereignty principle, Article 2(1) of the UN Charter and is grounded in customary international law. Germany is of the opinion that cyber measures may constitute a prohibited intervention under international law if they are comparable in scale and effect to coercion in non-cyber contexts.[59]

In broad terms, all the seven countries agreed that for an act to qualify as a prohibited intervention, it must fulfil two main conditions. Firstly, the act must bear on those matters in which states may decide freely, or in other words, interfere with the *domaine réservé of* another state. Secondly, the act must be coercive in nature.

---

53 Ministry of Foreign Affairs of Finland (2020) op. cit, p. 4.

54 Coco, A. Dias, T. (2021) *'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law*. European Journal of International Law, Vol 32(3), p. 787.

55 United Nations General Assembly (2015B) op. cit., p. 26.

56 Ministere Des Armees (2019) op. cit., p. 10.

57 United Nations General Assembly (2021A) op. cit., pp. 70, 71(c).

58 United Nations General Assembly (2015B) op. cit., pp. 26, 28(b).

59 The Federal Government (2021) op. cit., p. 5.

However, the definition of „*coercion*" remains unsettled among EU MSs. Some of the countries underline that an act involves coercion if its internal processes regarding aspects pertaining to its *domaine réservé* are significantly influenced and the act is specifically designed to compel the victim state to change its behaviour with respect to a matter within its *domaine réservé*.[60] Germany brings an example of a state spreading disinformation via the internet, and thereby deliberately inciting violent political upheaval, riots and/or civil strife in a foreign country, and thus significantly impeding the orderly conduct of an election and the casting of ballots.[61] Tampering with elections is also mentioned by other states.[62]

Others remain more cautious and state that for an act to include coercion, it should effectively deprive the target state of its ability to control or govern matters within its *domaine réservé.*[63] Here France brings an example: "*Interference by digital means in the internal or external affairs of France, i.e. interference which causes or may cause harm to France's political, economic, social and cultural system, may constitute a violation of the principle of non-intervention.*"[64]

However, it is generally accepted that merely influencing the other state by persuasion or propaganda, providing harsh criticism or causing nuisance with the aim of attempting to achieve a certain behaviour from the other state does not qualify as coercion.[65] Moreover, the acting state must intend to intervene in the internal affairs of the target state.[66] Finally, there has to be a causal nexus between the coercive act and the effect on the internal or external affairs of the target state.[67]

---

[60] Ibid. United Nations General Assembly (2021A) op. cit., pp. 25, 57. Ministry for Foreign Affairs and International Cooperation (2021) op. cit., pp. 4-5. Tallinn Manual 2.0, commentary to rule 66, para 19. Finland's approach to this issues is "*…done with the purpose of compelling or coercing that State in relation to affairs regarding which it has free choice (so-called domaine réservé)*„ Ministry of Foreign Affairs of Finland (2020) op. cit., p. 3.

[61] The Federal Government (2021) op. cit., p. 5.

[62] United Nations General Assembly (2021A) op. cit., pp. 25, 57, 77. Ministry of Foreign Affairs of Finland (2020) op. cit., p. 3. Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 5.

[63] Schmitt, M. (2017) op. cit., p. 318.

[64] Ministere Des Armees (2019) op. cit., p. 7.

[65] The Federal Government (2021) op. cit., p. 5. Ministry of Foreign Affairs of Finland (2020) op. cit., p. 3.

[66] The Federal Government (2021) op. cit., p. 5.

[67] United Nations General Assembly (2021A) op. cit., p. 77. Schmitt, M. (2017) op. cit., p. 320, para 24 (the exact nature of the causal nexus was not agreed on).

3.4 COUNTERMEASURES

The baseline view which can be deduced to be the opinion of minimum 21 EU MSs derives from AJP-3.20, which acknowledges countermeasures as legal remedies.[68] Apart from AJP-3.20, seven EU MSs have publicly expressed their views on the topic. Countermeasures are not mentioned in the UN GGE and OEWG reports.

All seven EU MSs echo the understanding expressed in AJP-3.20: that injured states have the right to take proportionate[69] countermeasures under international law in response to an internationally wrongful act. Such measures would otherwise be unlawful under international law. Several additional elements related to the interpretation of the legal regime on countermeasures are mentioned below.

Germany, Italy and France point out that the response to a wrongful cyber operation may involve digital means or not.[70] Netherland brings an example of a countermeasure: "*a cyber operation could be launched to shut down networks or systems that another state is using for a cyberattack*".[71] France states that in the event of a cyberattack against its information systems, state agencies may conduct cyberoperations, and "*on a case-by-case basis, and on a decision by the national cyber defence chain, such operations may be carried out in the framework of counter-measures*".[72]

All countries refer to limitations related to countermeasures. Italy, France and Estonia point out that countermeasures can be employed in response to internationally wrongful acts below the armed attack threshold. Netherlands posits that countermeasures are subject to strict conditions.[73] Italy, Estonia, Germany, Finland and France add that countermeasures are limited to the purpose of ensuring compliance with breached obligations.[74] Equally, Italy, Finland, Netherlands and France confirm that countermeasures must not amount to a threat, or use, of force

---

[68] NATO (2020) op. cit., footnote 36.

[69] E.g. in the wording of France: „*commensurate with the injury suffered, taking into account the gravity of the initial violation and the rights in question*". Ministere Des Armees (2019) op. cit., p. 8.

[70] Ministere Des Armees (2019) op. cit., p. 8. The Federal Government (2021) op. cit., p. 13.

[71] United Nations General Assembly (2021A) op. cit., p. 62.

[72] Ministere Des Armees (2019) op. cit., p. 8.

[73] Government of the Kingdom of Netherlands (2019) op. cit., p. 63.

[74] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 5. Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 7. Ministere Des Armees (2019) op. cit., p. 7. United Nations General Assembly (2021A) op. cit., p. 29. The Federal Government. (2021). op. cit., p. 13.

and must be consistent with other peremptory norms, as well as with human rights and humanitarian law.[75]

Countries also bring out issues which can be seen as challenging. Italy and France point out that "*the victim-[s]tate is generally required to call upon the [s]tate of origin to discontinue the wrongful act and to notify it of its intention to take countermeasures in response to wrongful cyber operations*", however, such requirement may not apply if immediate action is needed to enforce the rights of the injured state and to prevent further damage.[76] Netherland agrees that "*if immediate action is required in order to enforce the rights of the injured state and prevent further damage, such notification may be dispensed with*".[77] Italy also states that countermeasures may be problematic due to, for example, difficulties of "*traceability, assessment of breach in relation with the threshold of the diligence due, significance of the harm suffered.*"[78] Germany explains that "*[d]ue to the multifold and close interlinkage of cyber infrastructures not only across different [s]tates but also across different institutions and segments of society within [s]tates, cyber countermeasures are specifically prone to generating unwanted or even unlawful side effects. Against this background, [s]tates must be particularly thorough and prudent in examining whether or not the applicable limitation criteria to cyber countermeasures are met.*"[79]

Netherlands, Germany and Estonia underline the requirement that the injured state invoke the other state's responsibility, i.e. that the internationally wrongful act be attributed to a state.[80] Finland agreed with the importance of having adequate proof (which generally does not have to be disclosed) on the source of the offensive operation and state responsibility before resorting to countermeasures, while admitting that in certain circumstances it may be possible to attribute the hostile operation only afterwards.[81] The latter may be seen in contradiction with

[75] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 5. Government of the Kingdom of Netherlands (2019) op. cit., p. 63. Ministere Des Armees (2019) op. cit., p. 8.

[76] Ministere Des Armees (2019) op. cit., p. 8.

[77] Government of the Kingdom of Netherlands (2019) op. cit., p. 63.

[78] Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 7.

[79] The Federal Government (2021) op. cit., p. 3, 64.

[80] United Nations General Assembly (2021A) op. cit., pp. 29-30, 63. The Federal Government (2021) op. cit., p. 13.

[81] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 6.

the understanding that countermeasures should normally be taken while the wrongful act is ongoing.[82]

Estonia has expressed the view that among other collective responses, states which are not directly injured may apply collective countermeasures to support the state directly affected by the malicious cyber operation, while underlining that countermeasures applied should follow the principle of proportionality and other principles established within the international customary law.[83] France disagrees and states that "*collective counter--measures are not authorised*".[84] AJP-3.20 reflects the difference of opinions and posits that "*it is an unsettled area of the law whether international organisations or other states may conduct countermeasures on behalf of an injured state for unlawful acts that occur below the threshold of an armed attack.*"[85]

3.5 STATE RESPONSIBILITY AND ATTRIBUTION

State responsibility and attribution are complex issues which are sparking different opinions on the international arena. The 2015 and 2021 UN GGE reports affirmed that states must meet their international obligations regarding internationally wrongful acts attributable to them under international law.[86] This reflects a general understanding that when a state's cyber operation violates its obligations under international law, it constitutes an internationally wrongful act under the law of state responsibility. Internationally wrongful acts require two elements: 1) attributability to the state under international law, and 2) breach of an international obligation of the state.[87]

The 2015 and 2021 UN GGE reports also affirmed that states must not use proxies to commit internationally wrongful acts using ICTs and that the indication that an ICT activity was launched or otherwise originates

---

[82] Ibid.

[83] ERR News (2019) op. cit.

[84] Ministere Des Armees (2019) op. cit., p. 7.

[85] NATO (2020) op. cit.

[86] United Nations General Assembly (2015B) op. cit., 28 (f); United Nations General Assembly (2021C) *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. New York: United Nations General Assembly. Available from: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf [Accessed 14 January 2022] 71 (g).

[87] International Law Commission (2001) *Report of the International law Commission on the work of its fifty-third session, 23 April-1 June and 2 July – 10 August 2001, Official Records of the General Assembly, Fifty-sixth session, Supplement No.10.* Geneva: International Law Commission. Available from: https://legal.un.org/ilc/documentation/english/reports/a_56_10.pdf [Accessed 20 January 2022], Article 2.

from the territory or the ICT infrastructure of a state may be insufficient in itself to attribute the activity to that state.[88] This is expanded by several EU MSs who add that state responsibility can be established if the cyber operation was carried out by a state organ, a person or entity exercising elements of governmental authority, or non-state actor while being under instruction, direction or control by a state.[89]

Regarding attribution, the baseline EU approach is settled in the EU Cyberdiplomacy toolbox which outlines the core principles such as 1) not all measures require attribution; 2) attribution is a sovereign political decision by a state; 3) EU MSs can coordinate attribution at EU level. According to the EU, attribution could be established, based on an analysis of technical data and all-source intelligence, including on the possible interests of the aggressor. It must be noted that there is no international legal obligation to reveal evidence on which attribution is based prior to taking an appropriate response. MSs may employ different methods and procedures to attribute malicious cyber activities and different definitions and criteria to establish a degree of certainty on attributing a malicious cyber activity.[90]

Importantly, the application of the regime of targeted restrictive measures by the EU does not amount to attribution, which is a sovereign political decision taken on a case-by-case basis.[91] The UN GGE 2021 report adds that invocation of the responsibility of a state for an internationally wrongful act involves complex technical, legal and political considerations.[92]

Several EU MSs emphasize that there is no requirement for the state to make a public attribution.[93] France underlines that "*a decision not to publicly attribute a cyberattack is not a final barrier to the application*

[88] United Nations General Assembly (2015B) op. cit., 28 (e)(f); United Nations General Assembly (2021C) op. cit., 71 (g).

[89] United Nations General Assembly (2021A) op. cit., pp. 28, 61-62, 78-79. Ministere Des Armees (2019) op. cit., p. 10. The Federal Government (2021) op. cit., p. 11. underlining „effective control"; Finland mentions .. /.../ if acting on behalf of the State" Ministry of Foreign Affairs of Finland (2020) op. cit., p. 5.

[90] Council of the European Union. (2017) *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activity*. Brussels: Council of the European Union. Available from: https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf [Accessed 14 January 2022].

[91] Council of the European Union (2019) *Council Decision* concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Brussels: Council of the European Union. Available from: https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf [Accessed 14 January 2022]

[92] United Nations General Assembly (2021C) op. cit., 71 (g).

of international law, and in particular to assertion of the right of response available to [s]tates".[94]

3.6 INTERNATIONAL HUMANITARIAN LAW

There is consensus among EU MSs that International Humanitarian Law (IHL) applies to cyber operations during armed conflicts, which is the same position as put forth in the UN GGE 2021[95] as well as in AJP-3.20.[96] However, there are differing views primarily on neutrality, distinction between military and civilian objects and when a cyber operation constitutes an attack under IHL. Nevertheless, for the most part the EU MSs view the applicability of IHL in cyberspace during a conflict in a similar manner, which is perhaps not surprising as all EU MSs are parties to the four Geneva Conventions and at least Additional Protocols I and II.

Eleven EU MSs[97] have stated their views on the applicability of IHL to cyber operations during armed conflicts, out of which, three (Finland, Austria, and Ireland) are not NATO members. Out of these three, only Finland has published a detailed document on their national position[98], and while Ireland has stated its intention to release a similar document, currently their more detailed views on the subject are not known beyond that IHL applies in cyberspace.[99] Therefore, while silent NATO and EU MSs may be assumed agree with the AJP-3.20, the same cannot be said for the non-NATO members. Consequently, the "*silent*" non-NATO EU MSs

---

93 Ministere Des Armees (2019) op. cit., p. 10. Ministry of Foreign Affairs of Finland (2020) op. cit., p. 6. Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 5. United Nations General Assembly (2021A) op. cit., pp. 28, 61. The Federal Government (2021) op. cit., p. 12.

94 Ministere Des Armees (2019) op. cit., p. 11.

95 United Nations General Assembly (2021C) op. cit., p. 18.

96 NATO (2020) op. cit., p. 19.

97 Note that Ireland and Slovenia have expressed their view on this particular matter but have otherwise not published a detailed interpretation of international law applicable to cyber operations. Austria (2020) op. cit., pp. 2-3. Czech Republic (2020) op. cit., p. 4. Estonia (2021) op. cit., p. 1. Ministere Des Armees (2019) op. cit., p. 4, Ministry of Foreign Affairs of Finland (2020) op. cit., p. 7, The Federal Government (2021) op. cit., p. 1, Department of Foreign Affairs (2021) *Statement by Minister Coveney at the UNSC Open Debate on Cyber Security*. [online]. Available from: https://www.dfa.ie/pmun/newyork/news-and-speeches/securitycouncilstatements/statementsarchive/statement-by-minister-coveney-at-the-unsc-open-debate-on-cyber-security.html [Accessed 7 January 2022], Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 9. Slovenia (2021) op. cit., p. 2, United Nations General Assembly (2021A) op. cit., pp. 77-78, Government of the Kingdom of Netherlands (2019) op. cit., p. 5.

98 Ministry of Foreign Affairs of Finland (2020) op. cit.

99 Department of Foreign Affairs (2021) op. cit.

that have not explicitly stated their interpretations remain an unknown variable.

Another point of divergence is perceptible on dual-use objects, where France has a slightly different interpretation to AJP-3.20, the Tallinn Manual 2.0 (TM) and other EU MSs. Under the AJP-3.20, if an entity has both military and civilian uses ("*dual use*"), a "*careful analysis must be carried out to determine if they constitute a lawful military objective*" through losing their classification as a civilian object "*or otherwise offer a definite military advantage*".[100] This interpretation mirrors TM Rule 102 whereby if there is doubt regarding cyber infrastructure that is "*normally dedicated to civilian purposes*" being used to make an "*effective contribution to military action*" a determination of military use "*may only be made following a careful assessment*".[101] The disagreement flows from the ambiguity of whether Article 52 (3) of AP I, which contains a presumption of civilian usage, reflects customary law, with TM concluding that such a presumption only applies to individuals as noted in Rule 95 of the TM based upon Article 50 (1) of AP I.[102]

Considering that not all NATO MSs are party to Additional Protocol I, such as the United States[103], it unsurprising that AJP-3.20 mirrors the compromise wording of the TM. France in its national position upholds the presumption of Article 52 (3) of AP I, whereby in case of doubt, objects (just as individuals under 50 (1)) are presumed not to be used to "*make an effective contribution to military action*".[104] France emphasises its disagreement with the TM interpretation[105], and hence by extension, with the AJP-3.20. However, considering that the AJP-3.20 was published after the French national position, it remains to be seen if France continues to maintain its position. By contrast, Germany explicitly confirms that they agree with the TM Rule 102 regarding the careful assessment.[106]

---

[100] Op. cit., p. 21.

[101] Schmitt, M. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 448.

[102] Ibid, p. 424.

[103] International Committee of the Red Cross. *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.* [online]. Available from: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/States.xspxp_viewStates=XPages_NORMStatesParties&xp_treatySelected=470 [Accessed 7 January 2022).

[104] Ministere Des Armees (2019) op. cit., p. 14.

[105] Ibid.

[106] The Federal Government (2021) op. cit., p. 8.

Similarly, the qualification of data has been subject to discussion. France, Finland[107], Romania[108] and Germany[109] provided converging opinions whereby data, although intangible, may become a protected object or military objective, through the principle of distinction. France, for example, considers that „*the special protection afforded to certain objects extends to systems and the data that enable them to operate*"[110] and carved out some examples. Accordingly, „*given the current state of digital dependence, content data (such as civilian, bank or medical data, etc.) are protected under the principle of distinction*".[111] There was no opposing view in the positions reviewed, however states approach this issue cautiously.

Furthermore, France disagrees with the TM on the definition of a cyberattack, as under the French interpretation, a cyber operation may be classified as an attack under Article 49 of AP I even if there is no injury or loss of life or physical damage.[112] Instead, it is enough if the object is no longer able to provide the service it was intended for.[113] The German position mirrors the sentiment, albeit less overtly, as they do not explicitly state that they reject the TM's interpretation.[114] The German definition refers to "*harmful effects on communication, information or other electronic systems*" as well as "*or on physical objects or persons*", and thus mirroring the French interpretation whereby the physical damage, to either objects or persons, is not required.[115]

The Finnish position does not explicitly define a "*cyberattack*", but rather states that a cyberattack may amount to use of force under Article 2 (4) of the UN Charter or "*armed attack*" under Article 51 based on its consequences.[116] The Finnish position does not therefore explicitly either affirm or contradict the TM's Rule 92.[117] AJP-3.20 does not provide an exact definition of a cyberattack, as the discussion is focused mainly on when a "*cyber operation*" (which includes cyberattacks) would amount

[107] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 7.
[108] United Nations General Assembly (2015B) op. cit.
[109] The Federal Government (2021) op. cit., p. 8.
[110] Ministere Des Armees (2019) op. cit., p. 15.
[111] Ibid, p. 14.
[112] Ibid, p. 13.
[113] Ibid.
[114] The Federal Government (2021) op. cit., p. 8.
[115] Ibid.
[116] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 6.
[117] Ibid.

to an "*armed attack*" or "*use of force*". Therefore, there is not a definite consensus on the definition of a "*cyberattack*", and whether physical damage is required for a cyber action to be considered a cyberattack among the EU MS.

The final major point of divergence is the application of the law of neutrality. AJP-3.20 leaves it for the individual state to interpret and apply the law of neutrality.[118] There appears to be consensus, among the available positions of France, Italy, the Netherlands and Romania that the law of neutrality applies in cyberspace,[119] however, there is disagreement of what it entails. While it is agreed that neutral territory must be respected, by refraining from harming any infrastructure located on such territory, or using it to launch attacks, there is disagreement whether the neutral state must deny *any* access to its ICT infrastructure.

France considers that while a state may allow the belligerents to use its ICT network for communication, it must otherwise prevent "any use" of its ICT infrastructure.[120] By contrast, Italy emphasizes neutrality in treatment, whereby "*any action*" by a neutral state must be "*equally applied to all belligerents*", with an example that a state may not provide or deny access to its ICT infrastructure to one party only.[121] The Dutch position makes a similar statement,[122] whereby it can be concluded that there are two distinct positions on the topic, one for treating all belligerents equally and the French position of only allowing communication to pass through its ICT infrastructure and otherwise preventing any use of its ICT infrastructure by the belligerents. Considering there are relatively few positions available on the topic, as only four EU MSs have expressed their views, this specific issue lacks agreement.

3.7 USE OF FORCE

Among the EU MSs examined, there is a similar interpretation of the applicability of the prohibition on the use of force enclosed in Article 2(4) of the UN Charter. The examined EU MSs generally agree that cyber

[118] NATO (2020) op. cit., p. 22.

[119] Ministere Des Armees (2019) op. cit., p. 16, United Nations General Assemblv (2021A) op. cit., p. 78. Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 10, Government of the Kingdom of Netherlands (2019) op. cit., p. 5.

[120] Ministere Des Armees (2019) op. cit., p. 16.

[121] Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 10.

[122] Government of the Kingdom of Netherlands (2019) op. cit., p. 5.

operations may amount to "*use a force*" based on the consequences ("*scale and effect*") of the cyber operation, with the means being unimportant. There is also broad support to the interpretation that a cyber operation with sufficiently severe consequences may amount to not only a "*use of force*" but also an "*armed attack*", the latter being the gravest form of "*use of force*", thereby upholding an appreciable distinction.

AJP-3.20 interpretation is effectively the same, whereby cyber operations may amount to a use of force, or an "*armed attack*" if grave enough based on their scale and effect.[123] However, there is disagreement over whether a cyber operation that lacks material damage can amount to a "*use of force*", which is reflected in the careful wording of AJP-3.20. AJP-3.20 agrees that cyber operations "*generally would not*" amount to a "*use of force*" if they only create "*temporary disruptions or denials of service*".[124] Moreover, AJP-3.20 mentions that if part of a wider concurrent conventional attack, cyber operations that in isolation would not amount to a "*use of force*" such as a "*temporary denial of service*", could be classified as an "*armed attack*".[125] Thus, there is room for interpretation, albeit the doctrine appears to cautiously agree that a mere temporary loss of functionality on its own would not be sufficient, thereby mirroring the TM approach.[126]

France continues to uphold the view that material damages are not required, and that loss of functionality could be sufficient for a cyber operation to be deemed a "*use of force*".[127] France's position contains an interesting contradiction to both the TM and the *Nicaragua* case upon which the former's view was based on. The TM considers that "*merely funding*" a hacktivist group "*would not be a use of force*"[128], which mirrors the case's determination whereby a "*mere supply of funds /.../ does not in itself amount to a use of force*".[129] However, the *Nicaragua* judgement considers "*training and arming*" to "*certainly /.../ involve the threat or use of force*". Contrastingly, France posits that the "*financing or even training individuals to carry out cyberattacks against France*" may be seen as an example of a "*use*

[123] NATO (2020) op. cit., p. 20.
[124] Ibid.
[125] Ibid.
[126] Schmitt, M. (2017) op. cit., p. 337.
[127] Ministere Des Armees (2019) op. cit., p. 7.
[128] Schmitt, M. (2017) op. cit., p. 331.
[129] Judgement of 27 June 1986, *Nicaragua v. United States of America*. International Court of Justice, paragraph 228.

of force".[130] Therefore, France's national position subtly appears to communicate its disagreement with the Court's view in the *Nicaragua* case, by suggesting that training, arming and funding are all equivalent levels of action in terms of the "*use of force*" classification.

In Italy's view, which was published after AJP-3.20, the matter remains unresolved as it is stated that the notion that cyber operations which "*merely cause loss of functionality*" is "*a controversial one*".[131] Nevertheless, Italy does consider that due to the "*reliance of modern societies on computers*", the "*interruption of essential services*" which would not necessarily require physical damage, could justifiably be considered a "*use of force*".[132] Consequently, it is reasonable to conclude that while there is no definitive consensus on whether "*a mere*" loss of functionality may amount to a "*use of force*", such an interpretation *could* be justifiable in the opinion of at least some EU MSs.

3.8 SELF-DEFENCE

Majority of the EU MSs agree that the right to self-defence under Article 51 of the UN Charter applies in cyberspace and that cyber operations may amount to an armed attack that enables a state to exercise the said right.[133] Similarly, there is no apparent controversy over collective self-defence or responding to a cyber operation amounting to an armed attack via conventional kinetic means, provided they are necessary and proportionate.[134] However, controversies exist regarding exercising self-defence against non-state actors whose actions are not on behalf of any state and whether very severe non-material consequences of a cyber operation may amount to an armed attack.

The extension of the right to self-defence to non-state actors whose actions are not on behalf of any state, is arguably the most divisive of the controversial topics on self-defence. France outright rejects such an extension to non-state actors acting on their own accord, despite

[130] Ministere Des Armees (2019) op. cit., p. 7.

[131] Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 8.

[132] Ibid.

[133] Government of the Kingdom of Netherlands (2019) op. cit., pp. 8-9, The Federal Government (2021) op. cit., pp. 15-16, Ministrv of Foreign Affairs of Finland (2020) op. cit., pp. 6-7., Ministere Des Armees (2019) op. cit., pp. 6, 8. Estonia (2021) op. cit., pp. 7, 8-9, Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 9, NATO. (2020) op. cit., p. 20.

[134] Ibid.

in "*exceptional cases*" taking self-defence measures against "*quasi-[s]tate*" non-state actors such as ISIS.[135] However, it must be noted that France included the caveat of "*general practice*" which is shifting the interpretation of the law of self-defence, whereby self-defence against such non-state actors may become authorised.[136]

By contrast, Germany considers that non-state actors can commit "*armed attacks*", with reference to its views on the acts of Al-Qaeda and ISIS[137], in which it considered that states taking actions against such non-state actors are acting in self-defence.[138] Therefore, Germany appears to support the extension of self-defence to non-state actors acting on their own accord. The topic, however, appears to be a difficult one, for Finland avoids taking a definitive position. Despite stating that the right to self-defence arises from an armed attack attributed to a particular state, the attached footnote clarifies that non-state actors may possibly be capable of armed attacks, but the "*related questions of self-defence*" against such actors are "*too complicated to be discussed here*".[139]

Another issue of controversy lies with the thresholds for an armed attack. The German position lists as relevant factors only items that relate to material damages or injuries, including indirect deaths, as well as serious territorial incursions.[140] However, the French position also points out that a cyber operation may be categorised as an armed attack if it also causes "*substantial*" economic damage.[141] The Dutch position remains uncommitted as they refer to a lack of international consensus in the case of a lack of "*fatalities, physical damage or destruction*" but with "*very serious non-material consequences*" which seemingly could include economy damage.[142] The Italian position refers to cyberattacks comparable to conventional attacks that cause "*disruption in the functioning of critical infrastructure*"[143], and thereby not explicitly mentioning the economic consequences. Finland raises the question on how should the indirect and long-term impacts

[135] Ministere Des Armees (2019) op. cit.
[136] Ibid.
[137] The Federal Government (2021) op. cit., p. 16.
[138] Letter dated 10 December 2015 from the Chargé d'affaires a.i. of the Permanent Mission of Germany to the United Nations addressed to the President of the Security Council.
[139] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 7.
[140] The Federal Government (2021) op. cit., p. 15.
[141] Ministere Des Armees (2019) op. cit., p. 8.
[142] Government of the Kingdom of Netherlands (2019) op. cit., p. 9.
[143] Italy: Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 9.

of the cyber operation be considered in the case of potential classification as an armed attack.[144]

Therefore, the issue of economic damage amounting to an armed attack remains controversial. Moreover, further discussions about the extent to which long-term and indirect impacts of cyber operations when they are being classified as a potential armed attack appear to be warranted, as currently there is considerable uncertainty.

4. CONCLUSION

The goal of this article has been to give an overview of the current status of EU MSs' public statements on international law applicable to cyber operations, identify the domains of international law where convergence of views can be observed and, in some instances, also highlight some areas with notable differences.

The analysis of EU MSs' legal positions and relevant international documents (especially taking into account the AJP-3.20) revealed that while only nine out of twenty-seven EU MSs have published their detailed official views on the interpretation of international law applicable to cyber operations, there appears to be more consensus between the countries than evident at first sight. The EU MSs are heading towards a common position in many areas, and that beyond what has been agreed in the UN already. In addition to the already long-established strong standpoints on the general applicability of international law to state behaviour in cyberspace and the foundational role of human rights, the following baselines can be identified:

A) The relevance of the concept of sovereignty in cyberspace has been endorsed in the UN GGE and OEWG reports and mentioned by all nine EU MSs who have published their more detailed legal views. Considering the consensus reflected in AJP-3.20, there seems to be a broad agreement among 23 EU MSs regarding the interpretation of sovereignty as a standalone rule, entailing both rights and obligations.
B) Nine EU MSs' positions considered due diligence as a key issue, closely linked to the principle of sovereignty and state

[144] Ministry of Foreign Affairs of Finland (2020) op. cit, p. 6.

responsibility; however, the modalities of the application of the concept in cyberspace remain less than straightforward. The broad idea that countries should not knowingly support cyber operations has been expressed also in the UN GGE and OEWG reports, despite not employing the term "*due diligence*".

C) Seven EU MSs have publicly shared their views on prohibited intervention. It is generally agreed that the obligation prohibits states from intervening coercively in the internal or external affairs of other states. In broad terms, all the seven EU MSs agreed that for an act to qualify as a prohibited intervention, it must fulfil two main conditions. Firstly, the act must bear on those matters in which states may decide freely, or in other words, interfere with the *domaine réservé of* another state. Secondly, the act must be coercive in nature. The UNGGE 2021 and 2015 reports also mention the principle of non-intervention but do not go into greater detail.

D) The baseline view which can be deduced to be the opinion of 22 EU MSs is that countermeasures are acknowledged as legal remedies. Al seven EU MSs who have separately expressed their views echo the AJP-3.20 general position in outlining that injured states have the right to take proportionate countermeasures under international law in response to an internationally wrongful act. Such measures would otherwise be unlawful under international law. AJP-3.20 posits that collective countermeasures remain an unsettled area of the law.

E) State responsibility and attribution are complex issues which are sparking different opinions on the international arena. The 2015 and 2021 UN GGE reports affirmed that states must meet their international obligations regarding internationally wrongful acts attributable to them under international law, thereby also reflecting the de minimis agreement among the EU. The EU's baseline approach to attribution is outlined by the Cyberdiplomacy Toolbox.

F) Majority of the EU MSs agree that the right to self-defence under Article 51 of the UN Charter applies in cyberspace and that cyber operations may amount to an armed attack that enables a state to exercise the said right. Similarly, there is no apparent controversy over collective self-defence or responding to a cyberoperation

amounting to an armed attack via conventional kinetic means, provided they are necessary and proportionate.

G) The general consensus that IHL applies to cyber operations during armed conflicts, as confirmed by the UN GGE 2021 report, is supplemented by separate mentions in the domestic positions of several EU MSs. IHL-related questions are also addressed in the AJP-3.20, but many open issues remain.

However, drawing more concrete conclusions on the EU MSs' interpretation of international law applicable to cyber operations is limited due to the majority of EU MSs not having published their positions. It should be also underlined that national positions vary one the level of detail and include several blanks where the country's positions are not clearly expressed or in some instances, certain topics not mentioned at all. Therefore differences in national positions or states' silence on certain topics do not necessarily or not always signify oppositions. At the same time, lack of detail in discussing certain concepts may refer to strategic omissions which reflect domestic objectives and principles.

To move forward with the goal of a unified EU position, we suggest a three-step approach: a) clarifying domestic views, b) determining the common denominator, and c) engaging EU MSs in wider political discussions aimed at reaching decisions on a common EU position. However, drawing up a national position on the application of international law to cyber operations is not a trivial exercise. Although the overwhelming majority of EU MSs now show interest and engage in the UN discussions on international peace and security in the context of the use of ICT, it is likely that a more proactive stance could be advanced by targeted capacity building in this specific area. The European External Action Service (EEAS) already has some tools for this, and the European Security and Defence College offers several cyber-related courses to its network, but it still lacks a comprehensive and regular training on international law and cyber operations. Furthermore, besides the cyber-policy entrepreneur MSs, the EEAS could also intensively use all its relevant mandates to promote discussion and coordinate efforts in developing a common EU position.

And finally, there are topics where we can observe clear-cut oppositions where a common EU approach is unlikely in the near future. Examples include collective countermeasures, details related to IHL such as law of neutrality and the classification of "*use of force*" and "*armed attack*".

While reaching a substantial global agreement on different issues related to international law in cyberspace may not be viable in the near future, groups of like-minded countries such as the EU should continue working on their respective approaches. This may be seen as leading to certain fragmentation, but it also serves as an opportunity for building partnerships and synergies which will eventually drive further the discussions on international venues and serve as a role model for other regions.

LIST OF REFERENCES

[1] Association of Southeast Asian Nations (2018) *ASEAN Leaders' Statement on Cybersecurity Cooperation*, Singapore: Association of Southeast Asian Nations. Available from: http://setnas-asean.id/site/uploads/document/document/5b04cdc25d192-asean-leaders-statement-on-cybersecurity-cooperation.pdf [Accessed 14 January 2022].

[2] Austria (2021) *Comments by Austria on the Zero-Draft for the OWEG's Final Report*. Available from: https://front.un-arm.org/wp-content/uploads/2021/02/Austria-Comments-Zero-Draft-OEWG-19.02.2021.pdf [Accessed 14 January 2022].

[3] Coco, A. Dias, T. (2021) *'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law*. European Journal of International Law, Vol 32(3).

[4] Council of the European Union (2017) *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activity*. Brussels: Council of the European Union. Available from: https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf [Accessed 14 January 2022].

[5] Council of the European Union (2019) *Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Brussels: Council of the European Union.* Available from: https://data.consilium.europa.eu/doc/document/ST- 7299-2019-INIT/en/pdf [Accessed 14 January 2022].

[6] Czech Republic (2020) *Czech Republic Statement by Mr. Richard Kadlcak Special Envoy for Cyberspace Director Cyberseuciryt Department at the 2nd substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations*. New York: United Nations General Assembly. Available from: https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf [Accessed 14 January 2022].

[7] Department of Foreign Affairs (2021) *Statement by Minister Coveney at the UNSC Open Debate on Cyber Security*. [online]. Available from: https://www.dfa.ie/pmun/newyork/news-and-speeches/securitycouncilstatements/statementsarchive/statement-by-minister-coveney-at-the-unsc-open-debate-on-cyber-security.html [Accessed 7 January 2022].

[8] ERR News (2019) *President Kaljulaid at CyCon 2019: Cyber attacks should not be easy* weapon. Tallinn: ERR News. Available from: https://news.err.ee/946827/president-kaljulaid-at-cycon-2019-cyber-attacks-should-not-be-easy-weapon [Accessed 14 January 2022].

[9] Estonia (2021) *Estonian contribution on the subject of how international law applies to the use of information and communications technologies by states, to be annexed to the report of the Group of Governmental Experts on Advancing responsible state behaviour in cyberspace (2019-21).* Available from: https://ccdcoe.org/uploads/2018/10/Estonian_contribution _on_international_law_to_the_gge_may_2021_English.pdf [Accessed 14 January 2022].

[10] European Commission (2020) *Joint Communication to the European Parliament and the Council the EU's Cybersecurity Strategy for the Digital Decade*. Brussels: European Commission. Available from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 [Accessed 20 January 2022].

[11] G20 (2015) *G20 Leaders' Communiqué Antalya Summit, 15-16 November 2015*. Anatalaya:G20, Available from: https://www.gpfi.org/sites/gpfi/files/documents/G20-Antalya-Leaders-Summit-Communiqu--.pdf [Accessed 14 January 2022].

[12] Government of the Kingdom of Netherlands (2019) *Appendix: International law in cyberspace*. Available from: https://www.government.nl/binaries/government/ documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf [Accessed 7 January 2022].

[13] International Committee of the Red Cross *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.* [online]. Available from: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/States.xsp?xp_viewStates=XPages_NORMStatesParties&xp_treatySelected=470 [Accessed 7 January 2022].

[14] International Law Commission (2001) *Report of the International law Commission on the work of its fifty-third session, 23 April-1 June and 2 July – 10 August 2001, Official Records of*

the General Assembly, Fifty-sixth session, Supplement No.10. Geneva: International Law Commission. Available from: https://legal.un.org/ilc/documentation/english/reports/a_56_10.pdf [Accessed 20 January 2022].

[15] Judgement of 27 June 1986, *Nicaragua v. United States of America*. International Court of Justice, paragraph 228.

[16] Letter dated 10 December 2015 from the Chargé d'affaires a.i. of the Permanent Mission of Germany to the United Nations addressed to the President of the Security Council.

[17] Ministere Des Armees (2019) *International Law Applied To Operations in Cyberspace*. Paris: Delegation a l'information et a la communication de la defense. Available from: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf [Accessed 7 January 2022].

[18] Ministry for Foreign Affairs and International Cooperation (2021) *Italian Position Paper on 'International Law and Cyberspace'.* Rome: Ministry for Foreign Affairs and International Cooperation. Available from: https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf [Accessed 7 January 2022].

[19] Ministry of Foreign Affairs of Finland (2020) *International law and cyberspace Finland's national positions.* [online]. Available from: https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727 [Accessed 7 January 2022].

[20] NATO (2020) *Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace* Operations. Brussels: NATO Standardization Office.

[21] Nuclear Tests (Australia v. France), Judgment, I.C.J. Reports 1974.

[22] Organization of American States (2021) *AG/RES. 2959 (L-O/20) International Law.* Washington: Organization of American States. Available from: http://www.oas.org/en/sla/iajc/docs/AG-RES_2959_EN.pdf [Accessed 14 January 2022].

[23] Osula, A. (2021) *'Aligning Estonian and Japanese Efforts in Building Norms in Cyberspace', So Far, Yet So Close: Japanese and Estonian Cybersecurity Policy Perspectives and Cooperation*. Tallinn: International Centre for Defence and Security.

[24] *Pre-draft Report of the OEWG – ICT Comments by Austria.* Available from: https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf [Accessed 14 January 2022].

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

[26] Schmitt, M. (2020) *Noteworthy Releases of International Cyber Law Positions – Part I: NATO*, New York: Lieber Institute West Point. Available from: https://lieber.westpoint.edu/nato-release-international-cyber-law-positions-part-i/ [Accessed 14 January 2022].

[27] Slovenia (2021) *Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, Informal virtual meeting (18, 19 and 22 February 2021) Slovenia Statement*. Available from: https://front.un-arm.org/wp-content/uploads/2021/02/Slovenia-19-February-2021-FINAL.pdf [Accessed 14 January 2022].

[28] The Federal Government (2021) *On the Application of International Law in Cyberspace*. Berlin: German Federal Foreign Office. Available from: https://ccdcoe.org/uploads/2018/10/Germany_on-the-application-of-international-law-in-cyberspace-data_English.pdf [Accessed 7 January 2022], p.3.

[29] United Nations General Assembly (1999) *Resolution Adopted by the General Assembly [on the report of the First Committee (A/53/576).* New York: United Nations General Assembly. Available from: https://undocs.org/en/A/RES/53/70 [Accessed 14 January 2022].

[30] United Nations General Assembly (2013) *Resolution adopted by the General Assembly on 23 December 2015 [without reference to a Main Committee (A/68/L.26 and Add. 1)] 68/98.* New York: United Nations General Assembly. Available from: https://undocs.org/A/RES/68/98 [Accessed 14 January 2022].

[31] United Nations General Assembly (2015A) *Resolution adopted by the General Assembly on 23 December 2015 [on the report of the First Committee (A/70/455) 70/237.* New York: United Nations General Assembly. Available from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/457/57/PDF/N1545757.pdf?OpenElement [Accessed 14 January 2022].

[32] United Nations General Assembly (2015B) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: United Nations General Assembly. Available from: https://undocs.org/en/A/70/174 [Accessed 14 January 2022].

[33] United Nations General Assembly (2021A) *Official compendium of voluntary national contributions on the subject of how international technologies by States submitted by participating government experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established*

pursuant to General Assembly resolution 73/266. New York: United Nations General Assembly. Available from: https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf [Accessed 14 January 2022].

[34] United Nations General Assembly (2021B) *Open-ended working group on developments in the field of information and telecommunications in the context of international security*. New York: United Nations General Assembly. Available from: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf [Accessed 14 January 2022].

[35] United Nations General Assembly (2021C) *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. New York: United Nations General Assembly. Available from: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf [Accessed 14 January 2022] 71 (g).

[36] United Nations Office for Disarmament Affairs (2019) *Fact Sheet Developments in the field of information and telecommunications in the context of international security.* New York: United Nations Office for Disarmament Affairs. Available from: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf [Accessed 14 January 2022].

[37] United Nations Office for Disarmament Affairs. *Developments in the field of information and telecommunications in the context of international security.* New York: United Nations Office for Disarmament Affairs. Available from: https://www.un.org/disarmament/ict-security/ [Accessed 14 January 2022].

[38] Wright, J. (2018) *Cyber and International Law in the 21st Century*. London: Chatham House. Available from: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [Accessed 14 January 2022].