CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

International Legal Perspectives on Cyber Operations: A Common Baseline for NATO Allies

Dr Agnes Kasper and Karine Veersalu
NATO Cooperative Cyber Defence Centre Of Excellence

Forthcoming in NATO Legal Gazette Issue 44 'Legal Perspective on NATO and Fifth Generation Warfare'

About the authors

Agnes Kasper, PhD, is the Head of Law Branch at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). She is also a Senior Lecturer of Law and Technology in the Department of Law of the Tallinn University of Technology (TalTech). She is a co-author of the 'Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States' the collaborative project led by University of Exeter with NATO CCDCOE, Ministry of Foreign Affairs of Japan and Ministry of Foreign Affairs of Estonia. The views expressed in this article are solely those of the author and may not necessarily represent the views of the CCDCOE.

Karine Veersalu is a former law researcher at the NATO CCDCOE, where her work focused on the research and analysis of State positions and national cyber strategies, and supporting the development of the 'Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States.' She holds a bachelor's degree in law from Tallinn University of Technology and is completing her LLM at Lund University. The views expressed in this article are solely those of the author and may not necessarily represent the views of the affiliated institutions.

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited knowledge hub offering a unique interdisciplinary approach to the most relevant issues in cyber defence. The heart of the CCDCOE is a diverse group of international experts from military, government, academia, and industry, currently representing 39 nations.

The CCDCOE maintains its position as an internationally recognised cyber defence hub, a premier source of subject-matter expertise and a fundamental resource in the strategic, legal, operational, and technical aspects of cyber defence. The Centre offers thought leadership on the cutting edge of all aspects of cyber defence and provides a 360-degree view of the sector. The Centre encourages and supports the process of mainstreaming cybersecurity into NATO and national governance and capability, within its closely connected focus areas of technology, strategy, operations, and law.

The Tallinn Manual, prepared at the invitation of the CCDCOE, is the most comprehensive guide for policy advisers and legal experts on how international law applies to cyber operations carried out between and against states and non-state actors. Since 2010, the Centre has organised Locked Shields, the biggest and most complex technical live-fire cyber defence challenge in the world. Each year, Locked Shields gives cybersecurity experts the opportunity to enhance their skills in defending national IT-systems and critical infrastructure under real-time attacks. The focus is on realistic scenarios, cutting-edge technologies, and simulating the entire complexity of a massive cyber incident, including strategic decision-making and legal and communication aspects.

The CCDCOE hosts the International Conference on Cyber Conflict, CyCon, a unique annual event in Tallinn, bringing together key experts and decision makers from the global cyber defence community. The conference, which has taken place in Tallinn since 2009, attracts more than 600 participants each spring.

The CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation.

Table of Contents

Abstract 5

1. Introduction 6

2. Overall trends in NATO 7

3. Key areas of convergence 9

3.1 Application of international law 9

3.2 Sovereignty 9

3.3 Non-intervention 11

3.4 Use of force 12

3.5 Due Diligence 13

3.6 International Human Rights Law 14

3.7 State responsibility 15

3.7.1 Attribution 15

3.7.2 Responses 16

3.8 International Humanitarian Law 19

3.8.1 Attack in armed conflict 20

3.8.2 Military objectives 20

4. Conclusions 22

Abstract

The overall international legal framework has not changed in the last few decades. What has changed is the maturity of the discussion and understanding on how the existing rules apply to the use of information and communication technologies. The year 2024 marked a turning point, and now the majority of NATO Member States either have an individual national position or joined a common understanding on the application of international law in 'cyberspace'. Since cyber operations are often covert, classified, deniable, or technically ambiguous, and most applicable international rules are technology neutral, verbal and written practice, particularly these elaborate national and common positions, carry exceptional importance. This short article focuses primarily on areas where Allies agree, areas of convergence among NATO Member States, leaving the discussion of divergences for another occasion. Analysing the published national positions of Member States and the EU's common understanding, this article **maps out the convergence areas or a 'common baseline' within NATO**, which can be of immense value for furthering legal interoperability and doctrinal development in the field of cyber operations (particularly in the light of the ongoing review of the Allied Joint Doctrine for Cyber Operations, AJP 3.20), and can potentially serve as a foundation for a formally agreed NATO common position in the future. It is timely for NATO to take onboard the collective understanding of Allies about how international law applies to cyber activities.

1. Introduction

Legal scholarly debate about the 'Law of the Horse' emerged with the spread of information and communication technologies (ICTs) in the mid-1990s. Judge Frank H. Easterbrook argued that cyberspace does not call for an entirely new, specialized body of law, just as there would be no need for a distinct regime – the law of the horse – for the many cases involving sale, injury, care, etc. for horses. In his words, an attempt to do so would be 'doomed to be shallow and to miss unifying principles'.[1] In his seminal article and book, Lawrence Lessig famously countered that cyberspace does necessitate new legal considerations, though existing legal doctrines should remain as a starting point that may need to be reinterpreted or tailored to accommodate regulation of technical design.[2] Today, Easterbrook's and Lessig's debate (regarding domestic law) has settled on the agreement that new technologies should be governed by general, established rules, which may need adaptations. This suggestion is just as useful for international law, and since its general rules are technology neutral,[3] they remain valid for all technologies, as also confirmed in the Nuclear Weapons Advisory Opinion[4] of the International Court of Justice (ICJ).

The applicability of international law in cyberspace and cyber activities had been a matter of controversy until the mid-2010s. Discussions on responsible State behaviour in cyberspace have progressed through various global and regional fora, including initially at the United Nations (UN) Group of Governmental Experts (GGE) and later the UN Open-ended Working Groups (OEWG). In 2013, the GGE came to the landmark conclusion 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',[5] which was also endorsed by the UN General Assembly later that year.[6] While a marginal minority of States continue to put forward proposals for a new global cyberspace convention,[7] by today more than one hundred States[8] have expressed their positions in some form[9] on *how existing* international rules apply to cyber activities.

---

[1] Easterbrook, F.H. (1996) *Cyberspace and the Law of the Horse*, 1996 University of Chicago Legal Forum 207. Available at https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2147&context=journal_articles

[2] 'the Code' - Lessig, L. (1999). *The law of the horse: What cyberlaw might teach.* Harvard Law Review, 113:501, 501-546. Available at https://cyber.harvard.edu/works/lessig/finalhls.pdf

[3] Dapo Akande, Antonio Coco, Talita de Souza Dias, *Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies* (2022) International Law Studies.

[4] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226, paras 39, 85, 86.

[5] UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98 (24 June 2013).

[6] United Nations General Assembly, *Developments in the field of information and telecommunications in the context of international security* (adopted 27 December 2013) UN Doc A/RES/68/243.

[7] These include eg China, Cuba, Iran, Pakistan, and Russia.

[8] Key EU Messages, UN Open-Ended Working Group on the use of ICTs in the context of international security, 'Norms and International Law' (Statement on behalf of the EU and its Member States, 7 July 2025) https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/2025-07-07_OEWG_Cyber_July_2025_EU_Statement_Norms_and_International_Law_FINAL.pdf accessed 15 January 2026.

[9] Publishing a position may be done in a national context or collectively in a common position. Also, the format varies, States may give preference to speeches, UN Statements, standalone written documents or academic articles. See Chapter 5 on Format in Mačák, K., Dias, T., & Kasper, Á. (2025). Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States, pp. 125-147. Available at Handbook-on-Developing-a-National-Position-on-International-Law-and-Cyber-Activities_A-Practical-Guide-for-States.pdf

2. Overall trends in NATO

Many NATO Member States have issued national positions since 2012, and the 2014 Wales Summit Declaration, paragraph 72[10] established a landmark shift in NATO policy formally recognizing that international law applies in cyberspace.[11] Some Member States – being also part of the European Union (EU) – expressed their positions via the 2024 Declaration on a Common Understanding of International Law in Cyberspace adopted by the Council of the European Union.[12] The following table lists NATO Members that have issued an individual national position, indicating the year(s) of the document(s)(see Table 1). The table also notes NATO Member States that have not issued an individual national position to date, but are part of the EU's Common Understanding.

Member State	Public Position	Member State	Public Position	Member State	Public Position	Member State	Public Position
Albania	—	Finland	2020	Lithuania	EU only	Romania	2021
Belgium	2025	France	2019, 2021	Luxembourg	EU only	Slovakia	EU only
Bulgaria	EU only	Germany	2021	Montenegro	—	Slovenia	2026
Canada	2022	Greece	EU only	Netherlands	2019	Spain	EU only
Croatia	EU only	Hungary	EU only	N. Macedonia	—	Sweden	2022
Czechia	2020, 2024	Iceland	—	Norway	2021	Turkey	—
Denmark	2023	Italy	2021	Poland	2022	UK	2018–2022
Estonia	2019, 2021	Latvia	EU only	Portugal	EU only	US	2012–2021

Table 1. Overview of national and common positions relevant for NATO Allies. Source: Cyber Law Toolkit https://cyberlaw.ccdcoe.org

A comprehensive list of publicly available national and common positions on the application of international law to cyber operations, with additional analytical tools and links to the original texts, is maintained in the CyberLaw Toolkit, managed by the University of Exeter, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), and the National Cyber and Information Security Agency of the Czech Republic (NUKIB).[13]

Since cyber operations are often covert, classified, deniable, or technically ambiguous, and most applicable international rules are technology neutral, verbal and written practice, particularly the elaborate national and common positions, carry exceptional importance.[14] Existing national and

[10] North Atlantic Treaty Organization, *Wales Summit Declaration* (NATO, 5 September 2014) https://www.nato.int/cps/en/natohq/official_texts_112964.htm accessed 15 January 2026.
[11] While the 2014 Declaration and many other documents use the wording 'international law applicable in cyberspace' or similar, logically this may not be entirely correct, as activities are not taking place in cyberspace, but States rather use cyberspace, cyber measures or ICTs to create certain effects or to achieve various objectives. While observing this, the authors also acknowledge that national and common positions, as well as many other documents may opt for the use of this term. Terminology remains an unsettled issue to date.
[12] Council of the European Union, *Declaration on a Common Understanding of International Law in Cyberspace.* 15833/24 (18 November 2024). Available at https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf
[13] The CyberLaw Toolkit, at https://cyberlaw.ccdcoe.org hosts a collection of national and common positions.
[14] The precise legal significance of national and common positions is currently unsettled. During the three roundtable discussions co-organized by the authors in 2024, most State officials from the 46 participating States have considered two aspects: national positions can be seen as interpretation of treaty law (eg Un Charter or

common positions on international law and cyber activities cover a very wide range of legal issues, including views on the application of foundational rules and principles,[15] specialized regimes,[16] and the law of State responsibility,[17] etc. While these positions serve many functions,[18] they are also useful in mapping out areas of convergence, divergence, and possible gaps in the existing legal framework. Moreover, particularly the common positions are a testament to the possibility of constructive dialogue and progress that States have already made on reaching common understandings, despite legal differences. This short article focuses primarily on areas where Allies agree, areas of convergence among NATO Member States, leaving the discussion of divergences for another occasion. Analysing the published national positions of Member States and the EU's common understanding, this article **maps out the convergence areas or a 'common baseline' within NATO**, which can be of immense value for furthering legal interoperability and doctrinal development in the field of cyber operations, and can potentially serve as a foundation for a formally agreed NATO common position in the future.

The year 2024 marked a turning point, and now the majority of NATO Member States either have a national position or joined a common understanding on the application of international law in 'cyberspace'. However, two notes of caution are merited. First, the degree of granularity in the different positions varies, making it difficult to draw conclusions on issues where States have decided to remain silent. Second, this field is highly dynamic, and some States are reportedly developing their national positions (even if they have signed up for the EU common understanding)[19] or reviewing their existing positions.[20] Therefore, the findings in this study should be treated as a snapshot of convergences at the beginning of 2026.[21]

Geneva Conventions); and national positions can qualify as expressions of *opinio juris* or evidence of State practice (as in customary international law). Few participants suggested that national positions may 'double-count' as *opinio juris* and State practice. See more on this Chapter 1 on Motivations in Mačák, K., Dias, T., & Kasper, Á. (2025). Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States, pp. 18-21. Available at Handbook-on-Developing-a-National-Position-on-International-Law-and-Cyber-Activities_A-Practical-Guide-for-States.pdf

[15] Such as sovereignty, non-intervention, use of force, armed attack, due diligence, etc.

[16] Such as human rights law, international humanitarian law, international criminal law, etc.

[17] Including attribution, countermeasures, plea of necessity, etc.

[18] See Chapter 2 on Motivations in Mačák, K., Dias, T., & Kasper, Á. (2025). *Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States,* pp. 22-43. Available at Handbook-on-Developing-a-National-Position-on-International-Law-and-Cyber-Activities_A-Practical-Guide-for-States.pdf

[19] Eg during the writing of this article at the end of 2025, Belgium published its national views, while it is also part of the EU's common position.

[20] For example, Estonia is planning to revise its national position, as announced by Dr Rene Värk, legal director at Estonian Ministry of Foreign Affairs at the CyCon 2025 conference, in the plenary session 'From Theory to Practice Developing a National Position on International Law in Cyberspace" on 29th May 2025. Video available at https://youtu.be/_o93N97jhG0?si=TueLeQ5-2wyBStC1

[21] Full references to national and common positions are omitted, these can be found at the CyberLaw Toolkit available at https://cyberlaw.ccdcoe.org/wiki/List_of_articles#Common_and_national_positions

3. Key areas of convergence

3.1 Application of international law

All national positions of NATO Member States consistently affirm that international law applies to State uses of ICTs.[22] This affirmation, often found near the start of the position paper, usually contains a general acknowledgement of the UN GGE and OEWG processes and the conclusions reached therein, and a statement of the applicability of the UN Charter, international humanitarian law, and international human rights law, which are then further expanded upon in detail. NATO as an alliance has likewise affirmed, as early as in 2014, the baseline that 'international law, including international humanitarian law and the UN Charter, applies in cyberspace', recognizing that cyber operations could threaten collective security.[23] Moreover, the Allied Joint Doctrine for Cyberspace Operations (AJP-3.20) also recognizes that NATO cyber operations, and cyber operations contributed by the Member States on behalf of the alliance, are to be carried out in accordance with international law, including the UN Charter, international humanitarian law, and international human rights law.[24]

Thus, the general applicability of international law to cyber activities is not contested in and of itself, but it is rather *how* the established rules operate in practice that calls for further clarification. NATO Member States have maintained in their positions that *existing* international law is fit for governing the use of ICT's, with several States additionally, implicitly, or explicitly, adding that they do not see a need for new rules for this purpose.[25]

3.2 Sovereignty

All national and common positions on the application of international law to cyber activities, including those of the NATO Allies, address the principle of sovereignty in their statements. There is a general consensus that sovereignty as a core principle of international law applies to State use of ICTs.[26] However, cyberspace, in addition to a physical layer comprising hardware like computers, cables and physical infrastructure rooted in a State's territory, consists also of data flows, virtual networks and interconnected cyber-infrastructure that are not easily viewed through a strictly territorial lens.[27]

This can, therefore, pose novel challenges to the application of the 'traditional' concept of sovereignty in cyberspace. Questions remain regarding this principle's exact legal character – whether it is a standalone rule, the violation of which may give rise to State responsibility – a view reflected in the

---

[22] See eg the national positions of Belgium, Canada, Czechia, Denmark, Estonia, Finland, France, Germany, Italy, the Netherlands, Norway, Poland, Romania, Sweden, the UK, the US, as well as the common position of the EU.
[23] NATO, *Wales Summit Declaration* (Press Release, 5 September 2014), available at https://www.nato.int/cps/en/natohq/official_texts_112964.htm , para 72.
[24] NATO. (2020, January). *Allied Joint Doctrine for Cyberspace Operations (AJP-3.20, Edition A Version 1)*. NATO Standardization Office. Available at https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf , para 3.3.
[25] For States that have explicitly expressed this, see eg the national positions of Belgium, Czechia, Estonia (2021), Norway, Romania, Sweden, and the US (2012).
[26] UN General Assembly, *Draft Final Report of the Open-ended working group on security of and in the use of information and communication technologies 2021-2025,* A/AC.292/2025/CRP.1 (11 July 2025), paras 41(a) and (e).
[27] Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention* (Chatham House, 2019), pp. 13-15.

majority of the examined State positions,[28] or a principle which merely guides State interactions, but does not constitute a rule in itself capable of being violated.[29] While a further analysis of the divergence of these views is beyond the scope of this article, it still leaves open the question of how States should treat cyber operations that fall below the threshold of non-intervention and use of force.

Aside from the debate on the legal nature of the principle, a common denominator in the examined positions is that all Member States recognise that sovereignty should nevertheless be considered when conducting cyber operations.[30] Thus, this disagreement should not undermine the significant number of examples and practical criteria for violation of sovereignty to occur that States have expressed in their positions. This has created more predictability and transparency around what criteria they use in their operational planning to evaluate cyber operations that could potentially be considered as encroaching on their own or another States' sovereignty.

The accumulation of State and common positions now provides clearer guidance for identifying such thresholds of potentially wrongful conduct, and violation of sovereignty. While there is no agreement on the exact threshold for the necessary effects or harm, and many States have argued for a lower one,[31] there seems to be at least a broader understanding that at a minimum, cyber operations causing substantial harmful effects on the territory of another State, such as physical damage, injury, loss, or death would highly likely be regarded by most States as a breach of sovereignty.[32] At the same time, not all non-consensual cyber operations are considered unlawful – several States seem to generally agree that cyber operations that have negligible or *de minimis* effects would not constitute a violation of international law.[33] In any case, States agree that all incidents should be assessed on a case-by-case basis, taking into consideration their scope, scale, impact, and severity.[34]

---

[28] The majority of national positions issued to date converge in that a breach of a State's sovereignty may constitute a violation, giving rise to State responsibility. From NATO Member States, the positions that support this view include eg the national positions of Belgium, Canada, Czechia, Denmark, Estonia, Finland, France, Germany, Italy, the Netherlands, Norway, Poland, Romania, and Sweden, as well as the common position of the EU.

[29] This view is mainly embraced by the UK (see the UK's positions from 2018, 2021, and 2022), as well as supported by the US, that has consistently held in its earlier positions that 'there is not sufficiently widespread and consistent State practice (...) to conclude that customary international law generally prohibits such non-consensual cyber operations [falling below the threshold of prohibited intervention or use of force] in another State's territory.' In its most recent 2021 position, the US considers that 'in certain circumstances, one State's non-consensual cyber operation in another State's territory, even if it falls below the threshold of a use of force or non-intervention, could also violate international law,' but that remote cyber operations would not constitute a violation per se and that 'there is no absolute prohibition on such operations'.

[30] Since all examined positions consider sovereignty, it would be difficult to claim that in practice it should not be considered or it is somehow irrelevant, even if it is 'only' a principle. Also, both Canada and the UK, each a proponent of the two different approaches of treating sovereignty in cyberspace, have stated that the differing viewpoints should not prevent States from assessing and achieving a consensus on when particular conduct can constitute an internationally wrongful act. See the national positions of Canada, para 21, and the UK (2021), para 10.

[31] Several States reject the notion that the effects or harm need to amount to physical damage in order to constitute a violation of sovereignty, citing examples of ransomware that encrypts computers and disables the payment of pensions (Czechia); deletion or modification of data without resulting in physical damage or loss of functionality (Denmark, Finland, Norway, Sweden); non-physical software-related impairments (Germany); exercising investigative powers in a cross-border context (the Netherlands); blocking digital communication between public bodies and citizens to interfere with the delivery of social services (Norway); and theft, erasure or public disclosure of data (Poland). See also the national position of Belgium, which does not cite specific examples, but does affirm that 'It is not excluded that a cyber operation that takes place on the territory of another
State and does not cause loss of functionality or physical damage may nevertheless
violate the sovereignty of a state.'

[32] See eg the national positions of Belgium, Canada, Czechia, Denmark, Finland, France, Germany, Italy, the Netherlands, Norway, Poland, Romania, and Sweden.

[33] See eg the national positions of Canada, Czechia, Denmark, Germany, and the US (2016, 2021).

[34] See eg the national positions of Canada, Czechia, Denmark, Finland, France, Germany, Italy, Norway, and Sweden.

3.3 Non-intervention

Allies' positions converge on the view that the principle of non-intervention is a foundational principle of international law and, apart from the earliest statements, most positions elaborate on its nature, elements, and examples in detail. The precise terms used slightly vary; preferences are given both to use 'the principle of non-intervention' or 'non-intervention', and also the synonymous 'prohibition of intervention' or 'prohibition on unlawful intervention'. There is no difference in the content of the rule.

The prohibition of intervention stems from State sovereignty and the sovereign equality of States. It applies only to State conduct, but not to non-State actors, unless their conduct is attributable to a State. There is agreement that non-intervention is not only a principle, but it is a primary rule that is capable of being violated. Most States have unequivocally declared that it is part of customary international law.[35] Several positions refer to or cite the *Nicaragua judgement*[36] of the ICJ as legal authority supporting their reasoning.[37]

The prohibition of intervention is fully applicable to cyber activities. A breach of this rule may occur if two cumulative conditions are met: the conduct involves interference in the *domaine réservé*, or the sovereign affairs of the target State, and the conduct is coercive.

Several positions point out that the *domaine réservé* refers to matters within internal or external affairs of States, and list examples such as the choice to decide freely on political, economic, social, cultural systems, or the formulation of foreign policy. To further clarify the application of this rule in the cyber context, the majority of Member States specify cases which may be qualified as falling within the States' *domain réservé* in cyberspace, e.g., tampering with electoral processes using ICTs,[38] or interfering with cloud services or networks,[39] or, more generally, via cyber vector within the target State's territory or within its jurisdiction.

Interference must also be coercive to qualify as unlawful intervention under international law. However, coercion is not defined in international law. Therefore, the national positions are key to clarifying its actual meaning. Use of force can be one of the most serious forms of coercion. Several Allies point out that coercion is also distinguished from lower intensity influence operations, propaganda, public diplomacy, and other ways of persuasion, as these latter are insufficient to qualify as intervention.[40] This is not to say that all influence and disinformation operations fall outside of this category.[41] But what matters is certainly the consequences, or for some Member States, the intent and design of the measures to achieve coercive effect. [43] Therefore, as a common baseline for the Allies' positions, coercive interference needs to rise to the scale and effect that it deprives the target State the freedom of choice with regard to its sovereign affairs and a case-by-case assessment is needed. Virtually all

---

[35] See eg the national positions of Belgium, Norway, the US, and the UK, as well as the common position of the EU.
[36] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986.
[37] See eg the national positions of Belgium, Czechia, Denmark, Estonia, Finland, Germany, Sweden, the UK, and the US, as well as the common positions of the EU.
[38] See eg the national positions of Belgium, Canada, Norway, UK, US, Czechia, Denmark, Finland, Germany, Italy and the EU's common position.
[39] See the EU's common position.
[40] See eg the national positions of Canada, Czechia, Denmark, Finland, Germany, the Netherlands, Norway, Poland, Sweden, the UK and the US.
[41] See eg the national position of Germany '...but disinformation campaigns leading to scale and effect also may also amount to violation…'; Poland '...disinformation campaign with scale and effect also may…'.
[43] See the terms: 'coercive effect' used in the national positions of Canada and Estonia; 'methods of coercion' in the national position of Czechia; 'potential of compelling' and 'designed to have decisive impact' in the national position of Denmark; 'purpose to compel', 'but cyber measure must be of serious nature' in the national position of Finland; 'State's will manifestly bent' and reference to intention in the national position of Germany; 'coercive impact' in the national position of Italy; 'goal must be to effect' in the national position of the Netherlands; 'narrow rule', 'designed to coerce', includes attempts to interfere coercively in the national position of the US; 'directly or indirectly coercive interference' in the common position of the EU.

Allies agree that a cyber operation tampering with election systems of the target State can constitute prohibited intervention if it is attributable to a State.[44]

3.4 Use of force

The prohibition of the threat or use of force enshrined in Article 2(4) of the UN Charter is a peremptory norm of general international law, and it features in all of the examined national and common positions. The prohibition undoubtedly applies to the conduct of State actors in the cyber context. Allies' positions uniformly confirm that, in assessing when a cyber operation amounts to a use of force, the emphasis is on the effects and not the means of the operation. A cyber operation will fall within the scope of Article 2(4) if its consequences are comparable to those produced by a conventional use of force, such as death, injury, destruction, or significant physical damage. Examples repeatedly cited include cyber operations causing the malfunction or damage of critical infrastructure or leading to accidents such as the crash of an aircraft.[45] Many of the Allies are open to the interpretation that non-physical consequences[46] of cyber operations may also be taken into account in determining whether a cyber operation, potentially in combination with effects of other operations, crossed the threshold of the use of force.[47] All Member States agree that the assessment must be made on a case-by-case basis. Some

[44] See eg the national positions of Belgium, Canada, Czechia, Denmark, Finland, Germany, Italy, the Netherlands, Norway, Poland, Romania, the UK, the US and the reference to 'ICT systems, cloud-services and networks" in the common position of the EU.

[45] See eg the national position of Poland 'An action in cyberspace that leads to: a permanent and significant damage of a power plant, a missile defence system deactivation or taking control over an aircraft or a passenger ship and causing an accident with significant effects may be considered the use of force"; national position of UK (2018) 'If it would be a breach of international law to bomb an air traffic control tower with the effect of downing civilian aircraft, then it will be a breach of international law to use a hostile cyber operation to disable air traffic control systems which results in the same, ultimately lethal, effects"; national position of US (2012) 'Commonly cited examples of cyber activity that would constitute a use of force include, for example: (1) operations that trigger a nuclear plant meltdown; (2) operations that open a dam above a populated area causing destruction; or (3) operations that disable air traffic control resulting in airplane crashes".

[46] For some States this may also include also severe economic loss (see eg national positions of Denmark, Netherlands, Norway).

[47] See eg 'With regard to the precise interpretation of the term force and the question as to whether economic or political coercion can qualify as use of force, Denmark considers that it generally cannot be ruled out that acts of economic or political coercion can fall within the purview of Article 2(4) of the UN Charter if, for example, a cyber operation resulting in the malfunctioning of a State's financial system leads to significant economic damage" (national position of Denmark); 'A question has also been raised, whether a cyberattack producing significant economic effects such as the collapse of a State's financial system or parts of its economy should be equated to an armed attack. This question merits further consideration" (national position of Finland); 'France does not rule out the possibility that a cyberoperation without physical effects may also be characterised as a use of force" (national positions of France); 'While it is generally accepted that cyber operations resulting in material damage can constitute a use of force, we consider the qualification of cyber operations which merely cause loss of functionality a controversial one. The inclusion of such operations in the scope of the prohibition of the use of force, however, could be justified if one considers that, because of the reliance of modern societies on computers, computer systems and networks, cyber technologies have enabled States to cause the interruption of essential services without the need of physical damage" (national position of Italy); 'Armed force that has a real or potential physical impact on the target state is prohibited.' In the view of the government, at this time it cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as the use of force" (national position of the Netherlands); '[T]he use of crypto viruses or other forms of digital sabotage against a State's financial and banking system, or other operations that cause widespread economic effects and destabilisation, may amount to the use of force in violation of Article 2(4)" (national position of Norway); 'Modern societies have come to rely heavily on ICT which can be disrupted, its usage prevented or denied or its workings altered by a cyber operation without resulting in any physical damage. A cyber operation can have far-reaching adverse effects or cause severe interruption of daily life. Depending on the circumstances, the combined effects of several cyber operations could, taken together, be comparable to a kinetic use of force" (common position of the EU).

Member States refer to contextual[48] and further factors in such assessments and frequently point to, *inter alia*, the criteria of severity and immediacy of the effects as offered in the Tallinn Manual 2.0.[49]

A recurring theme in the positions is the references to the ICJ's jurisprudence concerning the use of force. Czechia, France, Germany, the Netherlands, Norway, Poland, Romania, and Sweden point to specific ICJ cases[50] and/or use citations regarding the thresholds of use of force and armed attack. Most States unequivocally distinguish between the two and follow the view of the ICJ that 'armed attack' is considered as the gravest form of the use of force, in other words a use of force does not always constitute an armed attack. Only the US' position indicates an alternative view, using the formulation 'use of force / armed attack', hence not distinguishing between the relevant thresholds, but also expressly recognizing that other States may disagree.[51]

3.5 Due Diligence

The issue of due diligence features in all examined positions and opinions converge that it refers to a standard of conduct that applies in the cyber context. Generally, this standard of conduct derives from two sources, first the principle formulated by the ICJ in the *Corfu Channel* case that it is 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'[52] Second, the 'no-harm' principle recognized in the *Trail Smelter* case[53], also reflected by the International Law Commission Draft Articles on Prevention of Transboundary Harm from Hazardous Activities.[54]

All Member States examine whether due diligence is also a binding rule, but they differ in their approaches and conclusions. While the 2021 UK and US positions conclude that due diligence does not currently constitute a binding obligation of international law,[55] Canada's position, which is rather ambiguous in this respect, also uses the terms 'should' and 'expectation', but not 'must' and 'obligation', which may signal the voluntary and non-binding nature of the norm.[56] Due diligence is currently recognized as a non-binding norm in the cyber context, and the UN General Assembly has endorsed both the 2015 and 2021 GGA reports, which elaborate on Norm 13 (c) that 'States should not knowingly

[48] See eg the national positions of Czechia, Denmark, Finland, France, Germany, the Netherlands, Norway and the US.
[49] See Rule 69 of the Tallinn Manual 2.0: these factors are a) severity, b) immediacy, c) directness, d) invasiveness, e) measurability of effects, f) military character, g) State involvement, h) presumptive legality. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2017.
[50] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986; Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996.
[51] This view is expressed in the 24 April, 2024 speech of Richard C. Visek, Principal Deputy Legal Adviser in the Office of the Legal Adviser at the U.S. Department of State, serving as the Acting Legal Adviser: 'Many States that have published views also agree that the inherent right of self-defense may be triggered by, and exercised through, cyber means. In this regard, it is important to recall that many States—although notably not the United States—distinguish between a use of force, which in their view may not give rise to the right to use force in self-defense, and an armed attack, which would". See Richard C Visek, The 2024 Arlin M and Neysa Adams Lecture: International Law and Cyberspace: Building Consensus (Temple Law Review, vol 97, no 1, Fall 2024) pdf at https://www.templelawreview.org/lawreview/assets/uploads/2025/01/Visek_International-Law-and-Cyberspace.pdf accessed 17 January 2026.
[52] Corfu Channel (United Kingdom v. Albania), Merits, Judgment, I.C.J. Reports 1949, para. 22.
[53] Trail Smelter (United States v. Canada), Arbitral Tribunal, 16 April 1938 & 11 March 1941, Reports of International Arbitral Awards (RIAA), vol. III.
[54] International Law Commission, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, 2001, U.N. Doc. A/56/10.
[55] See eg the national positions of the UK and the US.
[56] See eg the national position of Canada.

allow their territory to be used for internationally wrongful acts using ICTs'.[57] There remains, however, a lack of clarity regarding the legal character of due diligence also outside of the context of cyber activities,[58] and what States appear to really agree on is the importance of the due diligence and that the topic requires further study.[59]

However, the majority of Allies agree that due diligence is a binding obligation,[60] hence all of their positions confirm the existence of at least an expectation to take reasonable steps if a State is notified about harmful activities emanating from its territory. There is agreement on the key elements of due diligence. These include the expectation of certain standard of conduct (taking appropriate, reasonably available and feasible steps to address the harmful activity), but not necessarily a specific result by the State from whose territory the harmful activity emanates; prerequisite knowledge to trigger the expectation; no presumption of State responsibility for the harmful act itself; no expectation to monitor all ICT activities within a territory.

3.6 International Human Rights Law

There is a clear and established consensus among States that international human rights law applies to State uses of ICTs.[63] States therefore have both a negative duty to refrain from unlawful interference with human rights and a positive duty to protect individuals' rights, and these obligations apply online in the same way as offline.[64]

Member States acknowledge, however, that certain human rights are of particular relevance in the digital environment. Key issues that the Allies have consistently raised in their positions include the freedoms of expression and opinion,[65] the right to privacy,[66] the freedoms of assembly and association,[67] and the right to access information.[68] While these themes remain central, there also appear to be several emerging issues that States seem to be considering and increasingly incorporating into their national

[57] UN General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174 (22 July 2015), endorsed by UNGA Res 70/237 (23 December 2015); UN General Assembly, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc. A/76/135 (14 July 2021), endorsed by UNGA Res 76/19 (6 December 2021).
[58] See International Law Commission, *Report of the International Law Commission on the work of its seventy-fifth session*, UN Doc A/79/10 (2024)
[59] Mačák, K., Dias, T., & Kasper, Á. (2025). *Handbook on the Developing a National Position on International Law and Cyber Activities*. p. 92.
[60] See eg the national positions of Belgium, Czechia, Denmark, Estonia, Finland, France, Italy, the Netherlands, Sweden and the EU's common position.
[63] See eg UN Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, Resolution A/HRC/RES/32/13 (1 July 2016); UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* A/70/174 (22 July 2015); UN General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. A/76/135 (14 July 2021); See also NATO, *Warsaw Summit Communiqué.* (9 July 2016).
[64] See the Human Rights Committee, *General Comment No 31 [80]: The nature of the general legal obligation imposed on States Parties to the Covenant,* CCPR/C/21/Rev.1/Add.13 (26 May 2004); see also the national positions of Belgium, Canada, Czechia, Estonia, Finland, Italy, the Netherlands, Norway, Poland, Romania, Sweden, the UK, and the US, as well as the common position of the EU.
[65] See eg the national positions of Belgium, Canada, Czechia, Finland, Italy, the Netherlands, Norway, Poland, Sweden, the UK, and the US, as well as the common position of the EU.
[66] See eg the national positions of Belgium, Canada, Czechia, Estonia, Finland, Italy, the Netherlands, Norway, Poland, Sweden, and the UK, as well as the common position of the EU.
[67] See eg the national positions of Canada, Czechia, the Netherlands, Sweden, and the US, as well as the common position of the EU.
[68] See eg the national positions of Belgium, Czechia, Estonia, Finland, Italy, and the US, as well as the common position of the EU.

positions, such as the right of access to the internet,[69] and the role of non-State actors in relation to human rights in cyberspace.[70]

States generally accept that qualified rights may be lawfully restricted for legitimate aims like national security, public order, or combatting crime. At the same time, certain measures, including internet shutdowns and broad censorship, may not satisfy these standards, a point underscored by States including Romania and the United States.[71] Finally, while States affirm that international human rights apply online as they do offline, they recognise that the nature of cyberspace and new technologies pose unique challenges and raise complex issues of territory and jurisdiction, as digital conduct often transcends physical borders, leaving open the questions of how far States must act to ensure human rights protection beyond their borders.[72]

3.7 State responsibility

The national and common positions demonstrate a clear and unanimous agreement that the general rules of customary international law on State responsibility are fully applicable to State conduct in cyberspace. This well-established body of law is reflected in the International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA).[73]

An internationally wrongful act of a State in the cyber context requires two conditions:

- Conduct consisting of an action or omission that constitutes a breach of an international obligation of the State.
- The conduct is attributable to the State under international law.[74]

3.7.1 Attribution

All examined positions specifically address attribution and agree that the rules of attribution remain fully valid in cyberspace. It is pointed out that attribution may be technically challenging. However, this is a question of evidence, and not a lack of clarity of international law. Based on well-established customary international rules, a cyber operation is attributable to a State when carried out by its organs, by persons or entities empowered by the law of that State to exercise elements of governmental authority acting in that capacity, or by non-State actors acting on the instructions of, or under the direction or control of, that State. [76] It is central to the national and common positions that States cannot avoid legal responsibility for wrongful cyber acts by acting through proxies or non-State actors.

Several Member States emphasize that attribution in the legal sense—identifying a State as responsible for an internationally wrongful act—must be distinguished from technical identification of an actor and

[69] See eg the national positions of the Netherlands, Poland, Sweden, and the US.
[70] See eg the national positions of Czechia, Poland, Sweden, and the US.
[71] On restrictions, see eg the national positions of Czechia, the Netherlands, Poland, Romania, and the US.
[72] See eg the national positions of Canada, Czechia, Finland, the Netherlands, Norway, Poland, and the US.
[73] International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, U.N. Doc. A/56/10 (2001).
[74] ARSIWA Article 2.
[76] ARSIWA Chapter II - Attribution of Conduct to a State.

from political attribution or public statements assigning responsibility.[77] Legal attribution is a matter of international law; technical and political attributions involve factual, technical, and policy considerations.

There is broad consensus that decisions on attribution are sovereign prerogatives of States. A State may attribute cyber operations individually or collectively, and it has discretion to make such attribution public. Several States point out that international law imposes no obligation to disclose the evidence or basis upon which attribution is made, although States may choose to do so for political or cooperative purposes.[78] The absence of public attribution does not affect the application of international law or the existence of State responsibility.

Attribution determinations are based on the assessment of available information, which may include technical data, intelligence, and contextual factors such as the nature, effects, and circumstances of the operation. Absolute certainty is not required; still, some national positions point out the importance of a reasonable assessment – by the attributing State - of the facts under the circumstances.[79]

3.7.2 Responses

According to the *Lotus* presumption in international law,[80] sovereign States are free to act unless there is a specific prohibition. While this principle has evolved and States are often expected to justify their actions, especially where they act contrary to legal prohibitions, it is a useful starting point regarding State uses of ICTs, where the applicability or interpretation of certain rules is still unsettled. National and common positions mainly focus on acts and responses thereto that may amount to breaches of international law, specific thresholds of breaches, or when they are unfriendly, or concern expectations on how to settle their differences. Rarely do they directly elaborate on the many possible actions that are *not* prohibited by international law but rather set the limits.

3.7.2.1 Peaceful settlement

The obligation of States to settle their disputes peacefully is a foundational principle enshrined in Articles 2(3) and 33 of the UN Charter. It is a customary rule,[81] which requires States to seek resolution to their disputes through peaceful means, including by 'negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice' in order to safeguard international peace and security.[82] States have consistently affirmed in

---

[77] See eg the national positions of Canada '[a]ttribution in its legal sense is of course distinct from the technical identification (or technical attribution) of the actor responsible for malicious cyber activity, whether State or non-State, as well as from the public denunciation of the responsible actor (political attribution). Further, Canada believes that the public attribution of internationally wrongful acts engages various political considerations beyond technical and legal attribution"; Denmark '[t]he application of international law and State responsibility does not depend on public attribution"; Finland '[i]t is in this regard useful to distinguish identification as a technical operation from attribution as a legal operation. Identification may be technically challenging given the often covert nature of hostile cyber activities but this is without consequence to the legal rules of attribution"; US (2021) '[i]t is crucial, however, to distinguish legal attribution from attribution in the technical and political senses. States and commentators often express concerns about the challenge of attribution in a technical sense – that is, the challenge in light of certain characteristics of cyberspace of obtaining facts, whether through technical indicators or all-source intelligence, that would inform a State's policy and legal determinations about a particular cyber incident; also national positions of Czechia, Estonia, France, Germany, Italy, the Netherlands, Sweden, and the UK, as well as the common position of the EU.

[78] See eg the national positions of Czechia, the Netherlands, Sweden, the UK, and the US.

[79] See eg the national position of Estonia (2019) '[a]t the end of the day what is required from the attributing state, is not absolute certainty but what is reasonable'; and Italy '[a]lthough under international law there is no general obligation thereto, Italy stresses the importance of transparency: attribution of cyber wrongful activities should therefore be reasonable and credibly based on factual elements related to relevant circumstances of the case'.

[80] The Case of the S.S. 'Lotus" (France v. Turkey), Judgment of 7 September 1927, P.C.I.J. (ser. A) No. 10 (1927).

[81] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986. para 290.

[82] UN Charter, Article 33.

their national positions that this obligation applies equally to disputes arising in the context of State uses of ICTs – States must be committed to maintaining a peaceful ICT environment, and when faced with harmful cyber operations, seek a peaceful, rather than a retaliatory response which could risk escalation.[83] Nevertheless, several States explicitly specify that the duty to settle disputes by peaceful means does not preclude recourse to other responses available under international law, including self-defence in the case of an armed attack or by taking countermeasures, provided that the relevant requirements are met.[84]

3.7.2.2 Retorsion

There is common understanding among Allies that States may respond to malicious cyber operations, and it is generally implied that such responses, of course, include conduct that does not amount to violations of international law. Some positions emphasize this by including a statement on retorsions.[85] States agree that retorsions are lawful, but unfriendly acts that a State may take in response to harmful or undesirable conduct by another State, including malicious cyber operations.[86] Because they are lawful by definition, retorsions are always available as a response option, regardless of whether the triggering cyber activity was unlawful. They can be used both in reaction to unfriendly or harmful acts, and in response to internationally wrongful acts. Examples include the imposition of certain types of sanctions (i.e. those that do not amount to a violation of international law), the declaration that a diplomat is persona non grata,[87] or even public attribution[88] of hostile cyber operations.

3.7.2.3 Circumstances precluding wrongfulness: countermeasures, necessity, self-defence

In some cases, States may respond by taking measures that would otherwise violate international law. These responses are exceptions, and their wrongfulness is precluded, but for the prior violation of international law entailing State responsibility or, in case of invoking the plea of necessity, for a grave and imminent peril. National and common positions address countermeasures[89] and necessity[90] in the meaning of ARSIWA as well as self-defence[91] in the context of Article 51 of the UN Charter. There are several converging points regarding the scope, purpose, and procedural elements of these responses.

Countermeasures

All examined positions are in agreement that the purpose of countermeasures is strictly to induce compliance with international law, including cessation of the wrongful act and reparation. They may not be taken for retaliation, punishment, or retribution. States consistently affirm that countermeasures must comply with customary international law as reflected in the ILC Articles on State Responsibility and applicable limitations. Countermeasures must not involve the threat or use of force.

Countermeasures are temporary, must end once the responsible State returns to compliance, and must be directed only at the responsible State. As a current common baseline for the Allies, countermeasures are available to the injured State, although there is an emerging view that collective countermeasures

---

[83] See eg the national positions of Canada, Czechia, Estonia, France, Norway, and the UK, as well as the common position of the EU.
[84] See eg the national positions of Canada, Czechia, and Estonia.
[85] See eg the national positions of Belgium, Czechia, Denmark, Estonia, Germany, the Netherlands, Norway, Poland, the UK, and the US, as well as the common position of the EU.
[86] Ibid.
[87] See eg the national position of the Netherlands, Norway and US (2021).
[88] See eg the national position of Norway.
[89] All published positions address countermeasures.
[90] Addressed in the national positions of Czechia, Finland, France, Germany, the Netherlands, Norway, Sweden, and the US, as well as the common position of the EU.
[91] All published positions address self-defence.

may be permissible.[92] Countermeasures must be necessary and proportionate to the injury suffered and to the aim of inducing compliance.[93] They must respect peremptory norms (*jus cogens*) and must not breach fundamental human rights, obligations of a humanitarian character prohibiting reprisals, or the inviolability of diplomatic and consular premises and personnel.[94] They should be reversible to the extent possible.[95]

Member States agree that countermeasures may be taken by cyber or non-cyber means, and do not need to be symmetrical. Cyber countermeasures may respond to non-cyber wrongful acts, and vice versa. Before resorting to countermeasures, the injured State must in principle call upon the responsible State to comply,[96] which includes providing notification[97] (with some exceptions that apply in the cyber context),[98] and offer to negotiate,[99] giving an opportunity for the responsible State to cease its wrongful conduct.

Self-defence

There is agreement among Allies that a cyber operation may amount to an armed attack when its scale and effects are comparable to those of a kinetic armed attack.[100] Furthermore, Allies recognise that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack.[101] All examined national and common positions further affirm that the inherent right of self-defence under Article 51 of the UN Charter and customary international law applies to State uses of ICTs.[102] A State targeted by a cyber operation that constitutes an armed attack may exercise its right of individual or collective self-defence, subject to the same conditions that apply to other forms of uses of force. The responding State may use force in self-defence and is not limited to cyber means; both cyber and conventional (kinetic) responses are available. Conversely, a cyber

---

[92] 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 (see NATO, Allied Joint Publication 3.20: Allied Joint Doctrine for Cyberspace Operations, Edition A Version 1, 2020. p. 22). Also, eg national position of Estonia '[i]t is therefore important that states may respond collectively to unlawful cyber operations where diplomatic action is insufficient, but no lawful recourse to use of force exists. Allies matter also in cyberspace';
[93] See eg the national positions of Belgium, Canada, Denmark, Estonia, Finland, France, Germany, Italy, the Netherlands, Norway, Poland, Romania, Sweden, UK and US.
[94] See eg the national positions of Belgium, Czechia, Germany, Italy, the Netherlands, Poland and the EU's common position.
[95] See eg the national positions of Czechia, Denmark and the EU's common position.
[96] Art. 52(1)(a) ARSIWA
[97] Art. 52(1)(b) ARSIW
[98] Several national positions emphasize that certain procedural aspects, such as notification requirement, require further discussion in the cyber context. See eg national position of Canada '[t]he precise scope of certain procedural aspects of countermeasures, such as notification, needs to be further defined through State practice given the unique nature of cyberspace"; Czechia 'countermeasures may be undertaken without such prior notification"; Netherlands '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"; Norway '[c]ountermeasures may be taken without prior notification to the responsible State if providing such notification might reveal sensitive methods or capabilities or prevent the countermeasures from having the necessary effect"; Sweden 'it should be noted that this rule also allows for countermeasures without prior notification when urgent measures are needed to preserve the rights of the injured State"; UK (2018) 'we would not agree that we are always legally obliged to give prior notification to the hostile state before taking countermeasures against it";
[99] Art. 52(1)(b) ARSIWA.
[100] It has been stated in the 2014 NATO Wales Summit Declaration (para 72) that a cyber attacks, in some cases, may lead to the invocation of Article 5. The 2021 Brussels Summit Communiqué reaffirmed that a significant cyber attack could trigger Article 5. The examined national positions further clarify this point, specifically confirming that the right of self-defence is both individual and collective, and that the assessment whether a cyberoperation (or a campaign) reaches the threshold of armed conflict depends it's the scale and effect.
[101] 2021 NATO Brussels Summit Communiqué, para 32.
[102] See eg the national positions of Belgium, Czechia, Denmark, Estonia (2021), France, Germany, Italy, the Netherlands, Norway, Poland, Sweden, UK, US and EU's common position expressly referring to Article 51 of the UN Charter.

response may be used in self-defence against a kinetic armed attack. There is no requirement to respond in kind.[103]

The exercise of self-defence—whether cyber or kinetic—must comply with the customary international law requirements of necessity and proportionality.[104] Force may be used only when necessary to repel or end the armed attack, and response measures must not exceed that objective. The right of self-defence remains subject to relevant reporting obligations, including notification to the UN Security Council.[105]

Necessity

Most, but not all Allies[106] address when the plea of necessity can be invoked in the cyber context.[107] They emphasize that it is a narrow and exceptional justification, available only under strict conditions and to be assessed on a case-by-case basis.

The plea of necessity may be invoked under Article 25 ARSIWA only when the act is the only way for a State to safeguard an essential interest against a grave and imminent peril. The peril must be serious, imminent, and clearly established on the basis of the information reasonably available at the time, and the threatened harm need not already have materialized, nor must it necessarily be physical.[108] A key point is that the peril does not need to be attributable to a State. The invocation of necessity remains strictly limited in scope and duration, and available only when no other real alternative exists for addressing the grave and imminent peril.[109]

3.8 International Humanitarian Law

All examined positions of Allies are in clear alignment that International Humanitarian Law (IHL) fully applies to cyber operations during armed conflict.[110] Moreover, they agree that application of IHL neither legitimizes conflict nor militarizes cyberspace. On the contrary, IHL exists to limit the effects of armed conflict, which includes limits on conduct and use of capabilities (including cyber) by the parties. IHL also seeks to protect civilians, civilian objects, and other protected persons and objects, as well as to regulate the conduct of hostilities. Core principles and protections of IHL, e.g., humanity, distinction, proportionality, military necessity, precautions, and protection of civilians, apply equally in the cyber context. Some national positions further acknowledge that IHL limits cyber capabilities and require legal review of cyber or cyber-enabled weapons, means, and methods of warfare.[111]

---

[103] See eg the national positions of Canada, Czechia, Estonia, Finland, France, Germany, Poland and US (2021).
[104] See eg the national positions of Belgium, Czechia, Estonia, France, the Netherlands, Norway, Poland, Sweden, UK and EU's common positions.
[105] See eg the national positions of Belgium, France, Germany and Sweden.
[106] See the collection of national positions regarding the plea of necessity in the CyberLaw Toolkit available at https://cyberlaw.ccdcoe.org/wiki/Plea_of_necessity
[107] See eg the national positions of Czechia, Finland, France, Germany, the Netherlands, Norway, Sweden, and the US, as well as the common position of the EU.
[108] Ibid.
[109] Ibid.
[110] See a collection of relevant sections of national and common positions in the CyberLaw Toolkit, available at https://cyberlaw.ccdcoe.org/wiki/International_humanitarian_law_(jus_in_bello). This has also been agreed in the landmark resolution 'Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict' at the 34th International Conference of the Red Cross and Red Crescent in 2024, which was adopted by consensus. Further see eg Kubo Mačák, The First Humanitarian ICT Resolution: Ambitions and Limitations, 25 November, 2024, available at https://www.ejiltalk.org/the-first-humanitarian-ict-resolution-ambitions-and-limitations/
[111] See eg the national positions of Belgium, Canada, Czechia, France, Germany, and the US.

3.8.1 Attack in armed conflict

Allies' positions[112] affirm that cyber operations can constitute an 'attack' under IHL when conducted in the context of an armed conflict. A cyber operation is considered an attack in armed conflict, when it amounts to an act of violence against an adversary, whether offensive or defensive,[113] meaning that it is reasonably expected to cause injury or death to persons, or damage or destruction to objects, including harmful effects on cyber infrastructure or the systems that rely on it.[114] This determination is based primarily on the effects of the operation, not the means used. While definitions of harm may vary, there is growing agreement that physical harm, significant functional disruption, or destruction are central indicators.[115] Furthermore, while some Allies included language on 'reasonably foreseeable'[116] effects, as a minimum, in the definition of an attack, it remains unclear what precise types or what order effects, beyond the direct first order effects,[117] are relevant in determining whether a cyber operation amounts to attack in the meaning of IHL.[118]

Where a cyber operation qualifies as an attack, the same IHL rules and principles that govern attacks by kinetic means apply. This framework applies regardless of whether the cyber operation is offensive or defensive, and even where the relevant infrastructure is dual-use, i.e. shared between civilian and military sectors. Cyber operations that do not rise to the level of an attack are still subject to relevant IHL rules and general principles of the law of armed conflict, such as the general protection of civilians and the obligation to take constant care, if conducted in the course of an armed conflict.[119]

3.8.2 Military objectives

Examined positions of the Allies unanimously emphasize that the rules pertaining to the principle of distinction apply in the cyber context. Accordingly, attacks, including those by cyber operations, shall be limited strictly to military objectives. Indiscriminate attacks are prohibited, regardless of whether conventional or digital means are used.[120] Member States recognize that objects indispensable to the survival of the population, which are protected by Article 54 Additional Protocol I, may include ICT infrastructure, hence these are also protected.[121] It is not controversial that civilian ICT infrastructures and objects (e.g. computers, networked devices, etc.) with no military significance enjoy protected status. However, the infrastructure in cyberspace can often be dual-use, thus the context may require specific considerations. It is conceivable that acts of civilians carrying out cyber operations may be

---

[112] Many, but not all national positions address the threshold of 'attack' in the meaning of Article 49 of Additional Protocol I or corresponding customary international law. However, even those States that remained silent about attack in their national positions (see eg the national positions of Estonia, Finland, Poland and Romania), eventually addressed the issue via the EU common position.
[113] This corresponds to the definition of attack under Article 49 (1) of Additional Protocol I.
[114] See eg the national positions of Belgium, Canada, Denmark, France, Germany and the EU's common position.
[115] Some Allies, eg Denmark seem to take the view that a cyber operation amounts to an attack only if it is expected to lead to physical harm.
[116] See eg the national position of Canada, Czechia, Denmark, Sweden and UK.
[117] Effects can also be indirect, reverberating, intended, unintended, cumulative, cascading, sequential, parallel, collateral, immediate, short-term, long-term, etc.
[118] It needs a note that the ICRC expressly includes both foreseeable direct and indirect (reverberating) effects in determining whether a cyber operation constitutes an attack under IHL. Example: a cyber operation that disrupts a power grid could cut electricity to a hospital; if patients die as a result, those indirect deaths are part of what must be considered in deciding whether the operation amounts to an attack. See International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations during Armed Conflicts* (ICRC Position Paper, November 2019) 7–8.
[119] Mačák, K., Dias, T., & Kasper, Á. (2025). Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States, pp. 103-104. Available at Handbook-on-Developing-a-National-Position-on-International-Law-and-Cyber-Activities_A-Practical-Guide-for-States.pdf
[120] See the collection of national positions on this matter in the relevant pages of the CyberLaw Toolkit, including https://cyberlaw.ccdcoe.org/wiki/Military_objectives
[121] See eg the national positions of Belgium, Czechia, France and Romania,

characterized as direct participation in hostilities; in this case, the respective civilians would become legitimate military targets.[122]

It remains controversial how IHL applies to data as such, whether data can constitute an 'object', and on this basis, enjoy protections as civilian objects. A few States consider that cyber operations targeting data may fall within the scope of IHL when the operation qualifies as an attack in armed conflict, and in such case relevant limitations of the law of targeting (e.g. rules of distinction, proportionality, precautions) apply. However, several States note that the issue needs further considerations.[123]

[122] See eg the national positions of France, Germany and UK (2021). Further see Kubo Mačák, 'Will the centre hold? Countering the erosion of the principle of distinction on the digital battlefield' (2023) 105(923) International Review of the Red Cross 965, 970–977

[123] See eg the national positions of Denmark, Finland, France, Germany, the Netherlands, Poland and the US.

4. Conclusions

Allies conducting cyber operations, whether or not contributing cyber effects separately or on behalf of the Alliance,[124] must conduct them consistently with international law, as well as adhere to their own national laws, and, where applicable, other legal frameworks.

The overall international legal framework has not changed in the last few decades. What has changed recently in the last few years is that most Allies now have clear and public positions on how to interpret and apply the rules of this framework in using ICTs. By issuing national and common positions, NATO Member States now actively exercise their role in developing and clarifying international law insofar as these documents have legal value.[125]

Two implications of this are highlighted here. First, now that many States have expressed their positions, Allies need to take these into account when designing, planning, and conducting cyber operations. It is natural that NATO's cyber operations doctrinal and policy development should build on or even derive from the convergences in these positions.[126] Second, however, it is also necessary to account for the differences and where States have chosen to remain silent on specific issues, and it falls to States to identify how legal frameworks apply to State uses of ICTs, and publicly articulate and confirm these standards. Many questions remain in the national and common positions, and there is ample room for both deepening, and widening the discussion on both the convergences and divergences.

Further State practice and *opinio juris* are needed to clarify, for example, the thresholds for violations of sovereignty, non-intervention, prohibition of use of force, etc. Articulations of specific examples of incidents that States would likely consider a wrongful act under international law can reduce the margin of error for misinterpretation by others. This in turn creates more transparency, clarity, and predictability. Case-by-case analysis of cyber incidents that States can consider in their operational planning would also further mutual respect and solidify the expectations (rules) of the international community. Therefore, it is worthwhile to facilitate and support the processes that address the application of existing international law to cyber activities, be it development or revision of a national position, capacity-building on these topics, or scenario-based discussions and exercises for bridging interpretation gaps.

By now, most Allies have considered the issue of how international law applies to the State uses of ICTs. They have addressed this question individually, and some also collectively via the lenses of the EU. It is timely for NATO to take onboard the collective understanding of Allies about how international law applies to cyber activities.

[124] Eg in accordance with SCEPVA (Sovereign Cyber Effects Provided Voluntarily by Allies) mechanism, which refers to a framework within NATO for voluntary provision of cyber capabilities and effects by individual NATO member States in support of Alliance operations and missions.
[125] Mačák, K., Dias, T., & Kasper, Á. (2025). Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States. pp. 18-21.
[126] The NATO AJP 3.20 published in 2020 could not possibly have benefited from the now available national and common positions, as they mostly came around in later years.