Council of the European Union

Brussels, 18 November 2024
(OR. en)

15833/24

CYBER 334
COJUR 111
COPS 622

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
Subject:	Declaration on a Common Understanding of International Law in Cyberspace

Delegations will find in the annex the Declaration on a Common Understanding of International Law in Cyberspace, as approved by the Council at its meeting held on 18 November 2024.

ANNEX

Declaration by the European Union and its Member States on a Common Understanding of the Application of International Law to Cyberspace

Malicious behaviour in cyberspace from both State and non-State actors is increasing in scale, severity, sophistication and impact. This presents a major challenge and threat to the functioning of our societies, economies, and our way of life. It also affects critical infrastructure and hampers the efforts of States to fully grasp the economic, social and sustainable benefits of digitalisation and to narrow the digital divide. Additionally, the increasing frequency, scale and severity of ransomware attacks by malicious actors may have an impact on international peace and security. With emerging technologies significantly advancing the complexity of malicious cyber activities, and Information and Communication Technologies (ICTs) increasingly playing a central role in various conflicts, respect for and adherence to the United Nations framework of responsible State behaviour in cyberspace remain essential to maintaining international peace, security and stability.

The EU and its Member States reaffirm their full commitment to, and stress the importance of the full implementation of, the United Nations framework of responsible State behaviour in cyberspace, adopted by consensus by the United Nations General Assembly, which affirms inter alia that international law, in particular the UN Charter, international human rights law and international humanitarian law, fully applies to cyberspace. We underscore that this framework, grounded in the application of international law, should remain at the core of the efforts of the international community.

We will continue working with international partners to establish one single, permanent, inclusive, regular and action-oriented United Nations mechanism to implement and advance responsible State behaviour in cyberspace. We support the Cyber Programme of Action initiative, which will allow to further enhance the global common understanding of the UN framework of responsible State behaviour in cyberspace, build global capacities and strengthen international and multi-stakeholder cooperation in this field.

A better global common understanding of the implementation of the UN framework for responsible State behaviour in cyberspace and notably of how international law applies to cyberspace contributes to enhanced global cyber resilience and further transparency and predictability of, and accountability for, States' conduct in cyberspace. In that vein, the EU and its Member States continue to support third countries through training and capacity building on the implementation of the UN framework of responsible State behaviour in cyberspace, including on how to develop a national position on the application of international law to cyberspace.

We acknowledge that an increasing number of States have already developed and put forward their national and regional positions on the application of international law to cyberspace. To support finding further common understanding, the EU and its Member States have today presented their common understanding of a non-exhaustive set of legal elements on the application of international law to cyberspace in the Annex.

With this common understanding, we reiterate that international law, including international human rights law and international humanitarian law, is fit for purpose in this digital age. We show that it is possible to reach an understanding on a set of fundamental principles and rules of international law applicable to cyberspace, including State sovereignty, the principle of non-intervention, due diligence, the prohibition on the use of force, and compliance with the rules of international humanitarian law, international human rights law, the law of State responsibility and lawful State responses. We underscore that recognising the application of international humanitarian law in cyberspace does not lead to or encourage the militarization of cyberspace, nor does it legitimise cyber warfare.

Today we have conveyed our common understanding on a non-exhaustive set of legal elements, which complements and is without prejudice to current and future national positions of EU Member States as well as any future evolution of this common understanding on the application of international law to cyberspace. Looking ahead, we will continue to further develop, extend, update and share our understanding of the application of international law to cyberspace, at national, regional and international level, and encourage all UN Member States to do the same.

Annex

The European Union and its Member States reaffirm that international law, in particular the UN Charter, international human rights law and international humanitarian law, fully applies to cyberspace. We present below a non-exhaustive set of legal elements, which complements and is without prejudice to current and future national positions of EU Member States as well as any future evolution of this common understanding on the application of international law to cyberspace.

I. Rights and Duties of States

1. State sovereignty

State sovereignty is a core principle of international law. It ensures that States may choose and develop their political and social systems and pursue foreign policy. From State sovereignty flow certain rules and principles such as territorial or personal jurisdiction, immunity, and non-intervention. States are entitled to exercise territorial jurisdiction over persons, property and activities within their territories and in accordance with their obligations under international law.

States exercise territorial jurisdiction over Information and Communications Technology (ICT) infrastructure located in their territory, and persons engaged in cyber activities, within their territory.

The violation of the obligation to respect State sovereignty amounts to an internationally wrongful act, even if such a violation does not constitute a prohibited intervention or a prohibited use of force. A violation of the obligation to respect sovereignty may occur when a cyber operation, attributable to a State, infringes upon another State's territorial integrity or leads to interference with or usurpation of inherently governmental functions of another State.

2. Principle of non-intervention

The principle of non-intervention is a well-established rule of customary international law and is a corollary of sovereignty and the sovereign equality of all States. It prohibits a State from directly or indirectly intervening in the affairs of another State. An activity that is attributable to a State qualifies as a prohibited intervention if it coercively interferes with matters in which each State may decide freely as stated by the International Court of Justice in the *Nicaragua Judgement*[1]. Coercion could mean to compel another State to involuntarily pursue or forego a course of action.

Accordingly, coercive interference with ICT systems, cloud-services and networks on another State's territory or within its jurisdiction without its consent, within its *domaine réservé*, can constitute a prohibited intervention under international law if it is attributable to a State (see section II below).

3. Due diligence

Due diligence is a principle of international law that applies in the cyber context. In the *Corfu Channel Judgement,* the International Court of Justice ruled 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."[2]

Due diligence is an obligation of conduct, not of result. As States have jurisdiction over ICT infrastructure and individuals as referred to in Section 1 above, they are required to make efforts that this ICT infrastructure is not used by non-State or State actors for acts contrary to the rights of other States, once they know or ought to have known of such activities. States are required to take all appropriate and reasonably available and feasible measures, in the given context, to act against cyber operations that violate rights of another State under international law. The same duty applies for cyber activities within the territory or ICT infrastructure that they otherwise effectively control.

---

1 Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits, 27 June 1986, ICJ Reports, p. 14, at p. 208, para 205.

2 Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania), 1949 ICJ Reports, p. 4, at p. 22.

If a State does not act with due diligence in relation to cyber activities within or using ICT infrastructure located in, its territory, it may commit an internationally wrongful act. At the same time, the due diligence obligation does not require preventive monitoring of all cyber activities and ICT infrastructure in the territory of a State or within its effective control.

4. The prohibition on the use of force

Pursuant to Article 2(4) of the UN Charter and customary international law, the threat or use of force against the territorial integrity or political independence of any State or in any other manner inconsistent with the purposes of the UN Charter is prohibited. Aggression within the meaning of UNGA Resolution 3314 (1974)[3] falls within the scope of this prohibition.

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. Whenever the scale and effects of a cyber operation are comparable to those of a traditional kinetic use of force, it constitutes a use of force within the meaning of Article 2 (4) of the UN Charter, which is prohibited unless specifically justified.

The exercise of the right of self-defence against an armed attack in accordance with Article 51 of the UN Charter is an exception to the prohibition on the use of force (see section III 3 a). Furthermore, the use of force may be authorised by the UN Security Council in order to maintain or restore international peace and security under Chapter VII of the UN Charter. The use of force that takes place within the limits of the consent of the State in whose territory that force will be used does not violate the prohibition on the use of force. Moreover, the use of force does not always constitute an armed attack.

[3] United Nations General Assembly Resolution 3314, 14 December 1974.

5. Compliance with International Humanitarian Law

International humanitarian law (IHL) applies to cyber operations conducted in the context of an armed conflict, whether international or non-international in character[4]. Cyber activities may amount to attacks within the meaning of IHL, i.e. acts of violence against the adversary, whether in offence or defence. IHL rules, including the principles of humanity, military necessity, distinction, proportionality as well as the obligation to take all feasible precautions, which govern the conduct of hostilities and are of fundamental importance when cyber means and methods of warfare are employed in the context of an armed conflict.

Among these equally important principles, the principle of distinction requires the parties to a conflict to direct their military attacks only against military objectives and combatants[5]. Military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage. In the cyber context specific consideration may be required, since ICT infrastructure is often used for both civilian and military purposes. If an ICT system, network or infrastructure does not constitute a military objective it enjoys the protection as a civilian object. Indiscriminate attacks are prohibited under the conditions laid down in Article 51 of the First Additional Protocol to the Geneva Conventions[6].

The principle of distinction applies irrespective of whether the cyber attack is exercised in an offensive or a defensive context. Civilians must be protected against attacks, unless they take a direct part in the hostilities including by cyber means, as must be civilian objects.

---

4 Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135), point 71 (f).

5 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, Articles 48, 51(2) and 52(2).

6 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, Article 51.

6. Compliance with International Human Rights Law

States must comply with their obligations under international human rights law online just as offline[7]. States are under a negative obligation to refrain from acting in violation of human rights, as well as a positive obligation to actively protect the rights of persons within their jurisdiction against such violations. Human rights might be particularly at risk in the cyber context with regard to the freedom of opinion and expression, the right to privacy, the freedom to seek, receive and impart information, the freedom of peaceful assembly and association, the prohibition of discrimination and the rights of the child.

II. Attribution of conduct triggering State responsibility

Legal attribution is one of the constitutive elements of an internationally wrongful act, and consists of the attachment of a given action or omission to a State[8]. It is a prerequisite for invoking State responsibility. Under the customary international law rules on attribution, as reflected in the relevant chapter of the International Law Commission's Articles on the Responsibility of States for internationally wrongful acts (ARSIWA)[9], a State is responsible for the conduct of its organs. It is normally not legally responsible for the conduct of non-State actors not empowered to exercise governmental authority. However, under Article 8 ARSIWA, in situations where non-State actors act on the instructions or under the direction or control of a State, that conduct is attributable to the State. Conduct by non-State actors may also be legally attributed to a State if the latter acknowledges and adopts the conduct as its own, as stipulated in Article 11 ARSIWA. It is for the injured State to decide to invoke the international responsibility of another State, and for that purpose to attribute conduct of non-State actors to that State. Each individual State has the competence to decide whether to keep an assessment on attribution confidential or to make it public. However, a publication of the assessment on attribution is not required for the attribution of n act to a State under international law.

---

7 Human Rights Council, Resolution A/HRC/RES/20/8 of 16 July 2012.

8 ILC Articles on State Responsibility, commentary to Article 2, para 12.

9 Responsibility of States for Internationally Wrongful Acts 2001, reproduced in annex to General Assembly resolution 56/83 of 12 December 2001, and corrected by document A/56/49(Vol. I)/Corr.4 (»ARSIWA«).

III. States' responses

1. Peaceful settlement of disputes

As reflected in Articles 2(3) and 33(1) of the UN Charter, the parties to any dispute, especially if the continuance of that dispute is likely to endanger the maintenance of international peace and security, shall seek a solution by peaceful means. Peaceful means include diplomatic measures, recourse to negotiation, mediation, conciliation, arbitration, judicial settlement or any other peaceful means of dispute resolution of their own choice.

2. Retorsions

States may react to a wrongful cyber operation of another State by adopting retorsions. These are acts that are perceived as unfriendly, but which do not involve a breach of international obligations vis-à-vis the other State[10]. Examples of retorsions are the breaking off or limiting of diplomatic relations or other restrictive measures such as the reduction of economic or financial relations that are not in violation of international law.

3. Actions of which the wrongfulness is precluded

States may also react to cyber operations of another State by adopting actions that would depart from their international obligations, but whose wrongfulness is precluded under international law due to specific circumstances. These circumstances are reflected in Articles 20 to 25 ARSIWA and include the consent of the target State (Article 20 ARSIWA), self-defence (Article 21 ARSIWA), countermeasures (Article 22 ARSIWA), *force majeure* (Article 23 ARSIWA), distress (Article 24 ARSIWA) and necessity (Article 25 ARSIWA).

---

[10] International Law Commission (ILC), *Draft articles on responsibility of States for internationally wrongful acts, with commentaries* (ILC Yearbook 2001) Vol II Part Two, p. 128.

a) Self-defence

A State targeted by a cyber operation constituting an armed attack may invoke its inherent right of individual or collective self-defence, in accordance with the requirements for the exercise of that right laid down in Article 51 of the UN Charter. In order for a cyber operation to constitute an armed attack, the scale and effects of the operation must be comparable to those of a conventional kinetic attack. The extent of any damage or destruction of property (including ICT infrastructure) or injury or death of persons, including as an indirect effect, are among the relevant factors for assessing whether the scale and effects of the cyber operation are grave enough to characterise it as an armed attack. In order to constitute a lawful use of force in the exercise of individual or collective self-defence, the use of armed force in self-defence must comply with the requirements of necessity and proportionality.

When a State invokes the right of self-defence in response to an armed attack, it may ask other States to act in its support or on its behalf. The right of self-defence may thus be exercised collectively but only at the specific request of the victim State. All relevant rules and limitations of self-defence equally apply to collective self-defence. Within the European Union, pursuant to Article 42(7) of the Treaty on European Union, if a Member State is the victim of armed aggression on its territory, the other Member States have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the UN Charter[11]. This is without prejudice to the specific character of the security and defence policy of certain Member States and the commitments under the North Atlantic Treaty Organization for those States which are members of it and for whom it is the foundation of their collective defence.

[11] Treaty on European Union, Article 42(7).

b) Invocation of State responsibility

Based on Article 42 ARSIWA, the State which is injured by an internationally wrongful cyber operation of another State may invoke the responsibility of that State[12]. According to Article 48 ARSIWA, any State other than an injured State is entitled to invoke the responsibility of the responsible State, if the obligation breached is owed to a group of States including that State, and is established for the protection of a collective interest of the group; or if the obligation breached is owed to the international community as a whole.

c) Countermeasures

The injured State may resort to countermeasures in order to induce the former State to comply with its obligations under international law. Such countermeasures, be it in the cyber domain or not, are measures that would normally constitute a violation of an obligation under international law but whose wrongfulness is precluded because they constitute a response to a previous violation by another State[13]. Countermeasures must be consistent with the relevant rules of customary international law.

On substance, countermeasures must not affect: (a) the obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations; (b) obligations for the protection of fundamental human rights; (c) obligations of a humanitarian character prohibiting reprisals; (d) other obligations under peremptory norms of general international law[14]. States taking countermeasures are not relieved from fulfilling their obligations (a) under any dispute settlement procedure applicable between them and the responsible State and (b) to respect the inviolability of diplomatic or consular agents, premises, archives and documents. Countermeasures must be proportionate and reversible, and they must cease when the original violation ends[15].

---

12 ARSIWA, Article 42.
13 ARSIWA, Article 22.
14 ARSIWA, Article 50.
15 ARSIWA, Articles 51 and 53.

d) Necessity

A State may invoke necessity under Article 25 ARSIWA for precluding the wrongfulness of an act not in conformity with its international obligations if it is the only way for the State to safeguard an essential interest of that State against a grave and imminent peril and it does not seriously impair an essential interest of the State or States towards which an international obligation exists, or of the international community as a whole[16]. In the cyber context, an interest may be considered essential on account of the type of infrastructure actually or potentially targeted by a cyber operation and when that infrastructure is relevant for the State as a whole. However, a State may not invoke necessity if it has itself contributed to the situation of necessity or if the international obligation in question excludes the possibility of invoking necessity.

---

[16] ARSIWA, Article 25.