SLOVENIA'S POSITION PAPER ON THE IMPORTANCE OF INTERNATIONAL LAW IN CYBER SPACE

REPUBLIC OF SLOVENIA
MINISTRY OF FOREIGN AND EUROPEAN AFFAIRS

List of abbreviations

ARSIWA	Articles on Responsibility of States for Internationally Wrongful Acts
ECHR	European Convention on Human Rights
ECtHR	European Court for Human Rights
GGE	Group of Governmental Experts
ICC	International Criminal Court
ICJ	International Court of Justice
ICT	Information and communications technology
IHL	International Humanitarian Law
ILC	International Law Commission
OEWG	UN Open-ended Working Group
UN	United Nations
UNGA	United Nations General Assembly

PART I

I. General remarks

This position paper provides a non-exhaustive overview of Slovenia's position on the application of international law to cyber activities. For the purpose of this paper, cyber activities are understood as actions of States and non-State actors involving the use of information and communication technologies (ICT) and associated physical assets that have a direct or indirect impact on the digital or physical space. In this context, the term *cyber activity* encompasses any use or employment of cyber capabilities aimed at achieving objectives in or through cyberspace. In specific contexts involving structured actions with potential kinetic effects, such as use of force or IHL, the term *cyber operations* is used for precision.

Cyber activities relate to physical (ICT hardware and other infrastructure, including physical network elements and logical components (data, software, protocols etc.), and the social layer (real and virtual persona), which are independent but closely interconnected.

In light of the continuous evolution of science and technology, this position paper is subject to future revision and updating.

II. Introduction

Slovenia is fully committed to promoting respect for international law, including in relation to all cyber activities. Slovenia recognises the growing importance and influence of cyberspace activities within and beyond States' territories and the need to ensure efficient application of international law in this field.[1]

Slovenia notes that the applicability of international law to states' use of cyberspace has been reaffirmed by the UN Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, and by the UN Open-ended Working Group (OEWG).[2] Slovenia is of the view that applicable international law includes all branches of international law, including, among

[1] UNGA Res. A/RES/79/1 (2024): "The Pact for the Future", para. 33.

[2] 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/68/98 (2013), adopted by the UNGA Resolution A/RES/68/243; 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 (2015), adopted by the UNGA Resolution A/RES/70/237; Report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, UN Doc. A/75/816 (2021); 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 (2021); Report of the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025, UN Doc. A/77/275 (2022); Report of the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025, UN Doc. A/79/214 (2024); UNGA Res. A/RES/75/240 (2021); UNGA Res. A/RES/78/265 (2024); UNGA Res. A/RES/79/237 (2024).

others, the law on the use of force, international humanitarian law (IHL), international human rights law (IHRL), and the rules of international law of State responsibility.

Further articulation is needed primarily on how international law applies in cyberspace. Slovenia holds that cyberspace does not constitute a new legal domain but is rather a means to affect objects and persons in the existing domains (land, sea, air and space). Consequently, the principles and rules of international law pertaining to the latter must be applied in the context of cyberspace.

Slovenia wishes to contribute to the discussion on how international law applies in cyberspace by issuing the present national position.

III. Sovereignty

The fundamental legal principle of state sovereignty, a well-established principle of international customary law,[3] applies to States' activities in cyberspace.[4] States exercise territorial sovereignty over cyber infrastructure and individuals engaging in cyber activities within their territory, encompassing rights of regulation, enforcement and jurisdiction. Slovenia maintains that this sovereignty extends to all cyber infrastructure and activities, irrespective of whether such infrastructure is publicly or privately owned. Slovenia further maintains that whether a cyber activity violates sovereignty depends on its nature and impact, requiring a case-by-case evaluation.

Generally, a violation of sovereignty that results in physical damage or injury, temporary or permanent loss of functionality or an interference with or usurpation of inherently governmental functions of a state, with the intention to cause such harm is considered an internationally wrongful act[5], triggering the international responsibility of the State to which such cyber act is attributable. For instance, a cyber activity causing damage to or loss of functionality of a State's infrastructure is deemed a violation of territorial sovereignty. Unauthorised intrusions that affect data or services essential for governmental functions may also constitute a violation of sovereignty.[6]

IV. Principle of non-intervention

The principle of non-intervention, as a fundamental principle of international law firmly grounded in customary international law,[7] applies only to relation between states, or between states and international organisations, but not to relations between non-state actors and a State.

[3] UNGA Res. 2625 (XXV) '*The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States* (1970); Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). [1986] ICJ Rep 14, paras. 202, 205; Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda). [2005] ICJ Rep 168, para 164.

[4] UN GGE Rep A/68/98 (2013), para. 20; UN GGE Rep A/70/174 (2015), paras. 27-28, endorsed by UNGA Res. A/RES/70/237 (2015); UN OEWG Rep A/79/214 (2024), para. 37.

[5] As defined in ARSIWA, Articles 20–27.

[6] Tallinn Manual 2.0, Cambridge University Press 2017, Rule 4, para. 15.

[7] ICJ Nicaragua, paras. 191-192, 205; ICJ Armed Activities DRC v Uganda (2005), paras. 162-163.

The prohibition of intervention comprises two elements: interference with sovereign prerogatives, i.e. internal or external affairs or matters of an inherently governmental nature on which each State is permitted to decide freely, and coercion. A prohibited intervention therefore means direct or indirect interference by coercive means in the internal or external affairs of another State, including its economic, political, cultural and social system and foreign policy. Any act intended to eliminate or limit the targeted State's prerogatives constitutes a prohibited intervention.

Cyber activities rise to the level of a prohibited intervention under international law if they are comparable in scale and effect to intervention in non-cyber contexts. Coercive means are those that intentionally deprive a State of the ability to control, decide upon, or govern matters of an inherently governmental nature. Thus, the intervention as such should intend to effect a change in the behaviour of the targeted State. An example would be undermining a State's ability to provide critical services or manipulating a State's internal processes using cyber means.

In the cyber context, not every interference is to be considered an intervention. The element of coercion is requisite to qualify a cyber act of interference as a prohibited intervention. Coercion must be distinguished from other acts that would not qualify as such, for example criticism, imposition of restrictive measures, sanctions or other ways of exerting influence through peaceful or diplomatic means. What constitutes coercion in a cyber context requires a case-by-case assessment that takes into account the specific circumstances.

V. Prohibition of the threat or use of force

Article 2(4) of the UN Charter and customary international law prohibit the threat or use of force by a State against the territorial integrity or political independence of another State, or in any manner inconsistent with the purposes of the UN. This prohibition enjoys the status of a peremptory norm (*jus cogens*).[8] The material scope of the prohibition is not confined to less grave forms, e.g. violation of sovereignty or prohibited intervention, or to certain grave forms, e.g. armed attack. This prohibition applies to the use of force in any form, regardless of the weapons or means employed,[9] and therefore includes cyber operations.

In the cyber context, Slovenia maintains that it is not the means employed but the scale and effects of a cyber operation that determine whether it constitutes a prohibited use of force, exceeding a violation of sovereignty or a prohibited non-intervention. Thus, when assessing whether a cyber operation constitutes a violation of the prohibition of the use of force, its scale and effects must be evaluated in light of the relevant circumstances on a case-by-case basis, including but not limited to gravity of the act or acts concerned in

[8] ICJ Nicaragua (1986) paras. 175-176, 188-190; ICJ Armed Activities DRC v Uganda (2005), paras. 164-165.
[9] Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 226, para. 39.

terms of scale and effect rather than the means used.[10] A cyber activity would be qualified as a use of force if its scale and effects reached the same level as those of the use of force in non-cyber activities.[11] Accordingly, a cyber operation or a threatened cyber activity amounts to a threat to use force when the threatened activity, if carried out, would be a use of force.

Minor disruption of cyber activities alone does not amount to a use of force, whereas cyber operations causing physical damage or injury would ordinarily qualify as a use of force. Under certain circumstances, cyber operations producing exclusively non-physical effects may also constitute the use of force.

A valuable indicator that the threshold of the use of force has been met is the intentional targeting of critical infrastructure.[12]

Slovenia maintains that it will individually examine, on a case-by-case basis, those cyber operations that may constitute a threat or use of force, and will individually determine whether the 'scale and effects'[13] are such that a cyber operation amounts to a violation of the prohibition on the use of force, or whether the threatened activity constitutes a threat to use force.

VI. International humanitarian law (IHL)

The interpretation of the notion of 'attack' as understood under IHL / the law of armed conflict with regard to cyber operations is essential to the applicability of a number of IHL limitations and prohibitions. A cyberattack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons, or damage or destruction to objects. This includes any reasonably foreseeable consequential damage, destruction, injury or death. Slovenia considers that even a loss of functionality may qualify as an attack under IHL if it is sufficiently devastating in its effects. This position aligns with the widely accepted disregard for the types of weapons and means employed when assessing whether the threshold of an attack has been reached.

The rules and principles governing the conduct of the hostilities must also be respected in cyber-space.[14] IHL, together with its fundamental principles – including humanity, military necessity, distinction, proportionality and precautions – is applicable to cyber operations during armed conflict or occupation, if such operations are executed in the context of that conflict or occupation, or trigger the application of IHL in and of itself.[15] IHL also affords special protection to certain persons or objects, such as medical units

[10] UNGA Res. 3314 (XXIX) '*Definition of Aggression*' (1974), para. 2; ICJ Nicaragua (1986), para. 195; ICJ Armed Activities DRC v. Uganda (2005), paras. 163-164.
[11] According to the Tallinn Manual 2.0 (Rule 69 and accompanying commentary), a number of factors are relevant when assessing the scale and effects of a cyber operation, including the consequences of the cyber operation, whether the operation is military in nature and whether it is carried out by a state.
[12] There is currently no internationally agreed definition of critical infrastructure (CI). Therefore, it would be helpful to determine the scale and effects of the cyber activity.
[13] ICJ Nicaragua (1986), para. 195.
[14] Similarly, human rights are applicable offline as well as online. For more, see the text below.
[15] However, it is important to note that most cyber activities are not part of an armed conflict, which therefore excludes the use of IHL.

and transports, cultural property, the natural environment, works and installations containing dangerous forces and objects indispensable to the survival of the civilian population, among others. Slovenia maintains that affirming the application of IHL to cyber operations does not in any way legitimise cyber warfare or encourage the militarisation of cyberspace.

As different objects appear in cyberspace in comparison with physical space, the application of IHL extends to all components of cyberspace, including data. Slovenia is of the view that data do not qualify as objects, since an object is understood as something visible and tangible. Certain cyber operations against data are nonetheless prohibited. Civilian data are protected against cyberattacks in cases where tampering with, damaging or deleting such data would reasonably be expected to cause injury or death to persons, or damage or destruction to objects. Manipulation of data that would endanger the functioning of medical services, or impartial humanitarian organisations, is likewise prohibited.

The principle of distinction demands distinguishing between civilian objects and military objectives, and between civilians and combatants. The latter also include *levée en masse*, that is inhabitants of an unoccupied territory, who on the approach of the enemy spontaneously take up arms to resist invading forces without having time to form themselves into regular armed units. Owing to the opportunities presented by cyber warfare, resisting invading forces may include conducting military operations against objectives deep within enemy territory.

The protected status of civilians under IHL may, however, cease as a result of their engagement in acts of a cyber nature amounting to direct participation in hostilities. This may occur where civilians conduct offensive cyber operations intended to affect the enemy's military activity or capacity, or defensive operations intended to protect their own military objectives. Civilians participating in such actions should be made aware of the legal implications of their involvement, and of the rules and principles of IHL they are required to follow. Children must not be allowed to take a direct part in hostilities of a cyber nature.[16]

Slovenia is convinced that further work on the application of IHL in cyberspace should build on the existing legal framework, strengthening and promoting it while simultaneously acknowledging the challenges posed by cyberspace.

VII. International human rights law (IHRL)

Slovenia is fully committed to the realisation of human rights. IHRL also applies to cyber activities.

[16] UN Convention on the Rights of the Child (1989) Optional Protocol (2000) Arts. 1, 5.

States are obliged, to the same extent in both the physical and virtual world to respect, protect and fulfil the relevant human rights of individuals and the assumed human rights obligations, as set out in applicable human rights treaties and domestic law.[17]

All human rights may be affected by cyber activities. The rights that may be particularly exposed include the right to freedom of expression and conscience, the right to privacy, the confidentiality of communications, the protection of personal data, the right to freedom of assembly and association, and equality before the law. Subject to lawful derogations, restrictions and limitations, States must ensure the enjoyment of these rights without distinction, including in cyberspace, as confirmed by international jurisprudence.[18]

If a cyber activity results in a violation of human rights and is attributable to a State, the victim will, in principle, have recourse to complaints mechanisms available under applicable domestic law and treaties to which the State is a party. Slovenia supports the work of international human rights bodies and mechanisms that are developing adequate approaches to addressing the challenges of respecting, protecting and fulfilling State's human rights obligations in cyberspace.

Given that cyber activities may take place across the cyber infrastructure of multiple States, issues of competing jurisdiction may arise in cases of interference with human rights. Slovenia reiterates the position of the UN Human Rights Committee[19] regarding the extraterritorial application of human rights where a State exercises power or effective control beyond its territory, including functional jurisdiction where appropriate, with necessary adaptations for the cyber context.

VIII. Cybercrime

The Council of Europe (CoE) Convention on Cybercrime (ETS 185) and its Additional Protocols recognise the importance of common standards in defining cybercrime, regulating procedural powers for investigation and prosecution, and facilitating international cooperation in respect of cross-border cybercrime cases and the gathering electronic evidence abroad.

[17] The Right to Privacy in the Digital Age', General Assembly Res. 68/167, para. 3, UN Doc. A/RES/68/167 (December 2013).
[18] The European Court for Human Rights (ECtHR) also developed its practice in relation to violations of human rights in cyberspace. The ECtHR highlighted the importance of the positive obligation of the State to investigate online violations (criminal offence) of the victim's personality rights. The right to privacy was the focus of several cases of a State's intrusive secret surveillance and bulk interception, where the court established criteria for the required conditions for lawful interference and safeguards. In Wieder and Guarnieri (2023), for instance, it affirmed the applicability of the ECHR and its relevant Protocols to all extraterritorial surveillance activities, subjecting European intelligence agencies to the proportionality justification test when acquiring, processing or manipulating data of foreign individuals. The ECtHR has noted that user-generated content on the Internet provides an unprecedented platform for the exercise of freedom of expression and considered that the blocking of access to the Internet may be in direct conflict with the freedom of expression. In the inter-state case of Ukraine and the Netherlands v Russia (2022), the latter unsuccessfully claimed cyberattacks on the law firm instructing its council in the proceedings, attributable to the applicant States, thus alleging a lack of genuine application.
[19] General Comments 31 and 36 of the Human Rights Committee.

The Convention has a global impact because it was the first to establish clear standards in this field and because its application is not limited to CoE member states.

The UN Convention against Cybercrime (2024, not yet in force) addresses the issue of cybercrime at the global level and provides a framework for inter-state cooperation in crime justice and law-enforcement matters. In substance, it largely draws on the definitions contained in the Council of Europe Convention and is consistent with it, as well as with the UN Convention against Transnational Organized Crime.

PART II

I. State responsibility

Slovenia affirms that the general rules and principles of governing the responsibility of States for internationally wrongful acts – as reflected in customary international law and in the International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts (the ARSIWA)[20] – apply equally to State conduct in cyberspace.

A cyber activity may constitute an internationally wrongful act where the conduct is attributable to the State under ARSIWA and where the conduct constitutes a breach of an international obligation of that State. Where these elements are established, the responsible State incurs the legal consequences set out in ARSIWA – including cessation, assurances and guarantees of non-repetition, and full reparation.[21] Where the conduct amounts to a serious breach of an obligation arising under a peremptory norm of general international law, the special consequences provided for in ARSIWA also apply.[22]

The Republic of Slovenia further recalls that secondary rules contained in ARSIWA operate alongside the relevant primary rules of international law (including the Charter of the United Nations) and that the circumstances precluding wrongfulness, the rules on aid or assistance and on countermeasures are to be read together with the attribution and consequence rules when assessing State responsibility in the cyber domain.

A) Attribution of cyber activities

Slovenia recognises that attribution is essential to establishing State responsibility under international law and is therefore integral to the wider international responsibility framework used to guide legal remedies and collective political responses.

Slovenia affirms that existing international law, including the International Law Commission Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA)[23], applies in and to cyberspace.[24] Under ARSIWA, a cyber activity will constitute an internationally wrongful act only where (1) the conduct is attributable to a State under

[20] Text of the ILC Articles on the Responsibility of States for Internationally Wrongful Acts (2001) (ARSIWA), including the Articles cited above (Arts. 2, 4–11, 16–18, 20–31, 40–41).
[21] Military and Paramilitary Activities (Nicaragua v United States of America) — ICJ, Merits (1986) (leading exposition on attribution / 'effective control' and State responsibility practice).
[22] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) — ICJ, Judgment (2007) (discussing attribution, aiding/assistance and evidential standards in serious international wrongdoing).
[23] International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, in the *Report of the International Law Commission*, 53rd session, UN Doc A/56/10 (2001), Yearbook Vol II (Part Two)
[24] See also the guiding analysis in the *Tallinn Manual 2.0* on the International Law Applicable to Cyber Operations, which applies and interprets those principles in the cyber context; Michael N Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) ('Tallinn Manual 2.0') Rule 14 (on internationally wrongful cyber acts) (p 84) (non-binding expert commentary).

the ARSIWA attribution rules and (2) the conduct breaches an applicable international obligation.[25]

Slovenia observes that *political attribution* is a public policy judgement, based on the weight of available technical, intelligence and legal evidence and expressed with an assessment of confidence, intended to enable sanctions, diplomatic measures and coalition action. *Technical attribution* identifies forensic provenance and behavioural patterns (malware, IOCs, TTPs).[26] *Legal attribution* is a distinct legal determination that the facts establish a legal nexus sufficient for attribution under ARSIWA and may therefore give rise to obligations and remedies under international law.[27]

Slovenia considers that attribution may arise, inter alia, in accordance with the ARSIWA, from the conduct of State organs (Art. 4), persons or entities exercising governmental authority (Art. 5), organs placed at the disposal of another State (Art. 6), *ultra vires* acts of organs acting in an official capacity (Art. 7), conduct directed or controlled by a State (Art. 8), conduct of persons exercising elements of the governmental authority in the absence or default of the official authorities and in circumstances such as to call for the exercise of those elements of authority (Art. 9), or conduct acknowledged and adopted by a State as its own (Art. 11). Where a State provides infrastructure, assistance or direction with knowledge of the wrongful circumstances, derivative responsibility may also attach (Arts. 16–17).[28]

Slovenia notes that different adjudicative fora apply distinct control tests (notably the ICJ's *effective control* test in *Nicaragua*[29] and the ICTY's broader *overall control* formulation in *Tadić*[30])[31]; a claimant must identify the applicable standard and demonstrate the requisite factual nexus and the causal link between attributable conduct

[25] ILC, *Articles on Responsibility of States for Internationally Wrongful Acts* (ARSIWA) art 2; see arts 4–8, 11.

[26] By *malware,* we mean malicious software used to achieve intrusion, persistence, data exfiltration or disruption (e.g. binaries, scripts, payloads). *Indicators of compromise (IOCs)* are observable artefacts that reveal compromise or attacker infrastructure (e.g. IP addresses, domains, file-hashes, network indicators, or C2 endpoints). *Tactics, techniques and procedures (TTPs)* describe an actor's characteristic methods and behavioural patterns (the operational playbook by which attacks are executed). Technical attribution draws on these categories to establish provenance and link incidents to campaigns, but – while probative –such technical markers are not in themselves conclusive of legal responsibility. See Tallinn Manual 2.0 (Michael N Schmitt (ed.)), Rule 15 and accompanying commentary (pp 87–90) (on the role and limits of forensic indicators in attribution) and practical guidance on evidentiary presentation (pp 118–121).

[27] See *Tallinn Manual 2.0* on evidentiary and attribution guidance relevant to cyber operations; Michael N Schmitt (ed.), *Tallinn Manual 2.0* (n 27) Rule 15 (Attribution of cyber operations by State organs) and accompanying commentary (pp 87–90) (discussion of forensic indicators, evidentiary value of technical data and limits of provenance as proof of legal attribution).

[28] See United States Diplomatic and Consular Staff in Tehran (United States v. Iran) [1980] ICJ Rep 3 (Judgment of 24 May 1980) paras 69–75 (the Court records the United States' allegation of Iranian "complicity" and "approval" and examines the factual basis of State involvement). This material illustrates that State approval or endorsement may be relevant to the responsibility inquiry, but whether such conduct amounts to a legal "acknowledgement and adoption" depends on the concrete facts and degree of State engagement; by contrast, the ARSIWA formulation requires clear evidence that the State has "acknowledged and adopted" the act as its own, and subsequent jurisprudence has emphasised that post-hoc endorsement, promotion or reward will not necessarily satisfy that high threshold (see Makuchyan & Minasyan v Azerbaijan & Hungary, App No 17247/13 (ECtHR, 26 May 2020) paras 112–18).

[29] The Court explains the "effective control" threshold and that financing/equipping alone does not suffice to attribute acts absent of proof that the State "directed or enforced the perpetration" of the relevant operations; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) Judgment, ICJ, 27 June 1986, paras 115–16.

[30] Appeals Chamber formulation of the "overall control" test and discussion of how overall control may render a group's activities attributable to a State; *Prosecutor v Duško Tadić* (Appeals Chamber) Case No IT-94-1-A (15 July 1999) paras 120–23.

[31] The *Tallinn Manual 2.0* discusses these control standards and their application in cyberspace, and is a useful practical reference when mapping factual patterns to legal tests; Michael N Schmitt (ed.), *Tallinn Manual 2.0* (n 27) Rule 17 and commentary (pp 94–97) (discussion of attribution to non-State actors and the distinction between "effective control" and "overall control", and guidance on applying control tests in cyber cases).

and the injury alleged (see *Bosnia and Herzegovina v Serbia and Montenegro*[32] on causal nexus).

In the cyber context, States therefore rely on layered, mutually reinforcing evidence – technical forensics (logs, malware analysis, IOCs, TTPs)[33], intelligence assessments, behavioural analysis and documentary proof of direction, control or assistance – and publicly state the confidence level of their assessment while protecting classified sources and methods.[34]

B) Breach of international obligations

A breach arises where attributable State conduct in cyberspace contravenes a specific international legal obligation applicable to that State. Under ARSIWA, an internationally wrongful act requires (1) that the conduct be attributable to the State, and (2) that the conduct constitute a breach of an obligation in force for that State. In the cyber context, relevant primary rules may include – depending on the circumstances – the prohibition on the use of force[35], the principle of non-intervention[36], the duty to respect State sovereignty[37], treaty obligations, and applicable human-rights obligations. Whether a particular primary rule is engaged depends on the scale, effects and context of the operation. Establishing a breach therefore requires legal qualification of the attributable conduct against the identified primary rule(s) and, where remedies are sought, demonstration of the causal link between the attributable conduct and the injury or loss alleged.[38]

For the purposes of a public attribution statement, the Government's legal assessment is based on the balance of available evidence – including technical forensic data (system

[32] The Court emphasises the need for a "sufficiently direct and certain causal nexus between the wrongful act … and the injury suffered" when establishing responsibility and reparations; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* (Merits) Judgment, ICJ, 26 Feb 2007, para 462.

[33] By *logs,* we mean system and network-generated records used in forensic reconstruction (e.g. host/event logs, firewall/proxy logs, packet captures and other time-stamped records showing connections, processes and system events). *Malware analysis* refers to static and dynamic examination of malicious code (reverse engineering, sandbox execution and behavioural analysis) to identify capabilities, coding artefacts and reuse. *Indicators of compromise (IOCs)* are observable artefacts that reveal a compromise or attacker infrastructure (e.g. file-hashes, IP addresses, domain names, SSL certificates, registry keys). *Tactics, techniques and procedures (TTPs)* denote characteristic behavioural patterns and operational methods used by an actor (the "how" of intrusions that links incidents to campaigns). These technical categories are probative for provenance and linkage but, as the Tallinn Manual 2.0 explains, are indicia rather than by-themselves determinative of legal attribution; technical evidence should be presented as part of a layered, corroborated record together with intelligence and documentary proof. See Tallinn Manual 2.0 (Michael N Schmitt (ed.)), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) Rule 15 (pp 87–90) and practical evidentiary guidance (pp 118–121).

[34] These layered evidentiary approaches are consistent with the practical guidance set out in *Tallinn Manual 2.0* on compiling and presenting attribution evidence in cyber incidents; Michael N Schmitt (ed.), *Tallinn Manual 2.0* (n 27) (see especially the practical guidance on evidence and presenting attribution assessments, including recommended categories of unclassified disclosure and partner briefings) (pp 118–121).

[35] UN Charter Art.2(4) (prohibition on the use of force); see also Michael N Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) (non-binding expert commentary) (discussing the scale/effects approach to use of force in the cyber context).

[36] See *Military and Paramilitary Activities (Nicaragua v United States of America)* (Merits) Judgment, ICJ, 27 June 1986 (discussing the principle of non-intervention and related state obligations).

[37] See *Corfu Channel (United Kingdom v Albania)* (Merits) Judgment, ICJ, 9 April 1949 (on State sovereignty and respect for territorial integrity); see also the discussion of sovereignty and non-intervention in Tallinn Manual 2.0 (n 49).

[38] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* (Merits) Judgment, ICJ, 26 Feb 2007, para 462 (on the need for a sufficiently direct and certain causal nexus between wrongful conduct and injury for reparation).

and application logs; malware analysis), correlation of tactics, techniques and procedures (TTPs), intelligence reporting (including intercepted communications and human-source reporting where appropriate), evidence of State direction, control or material support, and any corroborating public or open-source material – and an evaluation that, taken together, this body of evidence is sufficient to establish a breach of the identified international obligation(s).[39]

C) Due diligence

States are under an obligation not to knowingly allow their territory or objects, activities and infrastructure under their jurisdiction to be utilised for actions that infringe upon the rights of other States.

The due diligence principle requires a State to take feasible measures with respect to cyber activities if it is aware, or ought to have been aware, of an act contrary to the rights of a victim state originating from, or routed through, its territory. If States do not have the ability to end such cyber activity, they should do their utmost to mitigate it and warn the target State. The due diligence principle does not encompass an obligation to take preventive steps to ensure that a State's territory is not used in a way that negatively affects the rights of other States. States are only required to exhibit due diligence, and thus to take reasonable measures to terminate or mitigate cyber activities that are reasonably likely to result in serious adverse consequences.

D) Circumstances precluding wrongfulness

Slovenia maintains that circumstances precluding the wrongfulness of a cyber activity include consent, self-defence, countermeasures, necessity, force majeure and distress.

Self-defence

If a cyber operation constitutes an *armed attack* – that is, a cyber operation that elevates to the level of cyber armed attack – then the targeted State may invoke its inherent right to use force in self-defence, individually or collectively, as recognised under Article 51 of the UN Charter and customary international law.[40] An armed attack should be distinguished from other forms of the use of force. The threshold of scale and effects to be met is higher than for less grave forms of use of force, and, consequently the material scope of corresponding right to self-defence is narrower.[41]

[39] On evidentiary categories and practical presentation of attribution evidence in cyber incidents, see Tallinn Manual 2.0 (n 2) Rule 15 and accompanying commentary (technical indicators, TTPs and limits on provenance as conclusive proof) and the practical guidance on compiling and presenting evidence (pp 118–121); see further ILC (n 26) arts 16–17 (aid/assistance; direction and control — knowledge and control elements).
[40] Tallinn manual 2.0, Rules 71-76 and accompanying commentary.
[41] ICJ Nicaragua (1986), paras. 50, 74, 176-181, 193-201, 210-211, 232-234, 238; ICJ Armed Activities DRC v Uganda (2005), paras. 118, 128, 142-143, 144-146.

A cyber operation that seriously injures or kills a number of persons, or that causes significant damage to, or destruction of, property, such as an attack on an air-traffic control system leading to a crash, or an attack on critical infrastructure causing serious physical damage, would constitute an armed attack, as its scale and effects would be similar to an armed attack executed with conventional weapons. A series of cyber activities, which individually do not reach the threshold of an armed attack, could be categorised as such if the accumulation of their consequences, taken together, meets the requisite scale and effects. A cyber operation of foreign origin, attributed to a State, international organisation or non-State actor, that does not meet the standard of an armed attack, does not entitle the victim State to invoke the right of self-defence.

Countermeasures

If a State is the victim of a malicious cyber operation that is attributable to a perpetrator State, the targeted State may be able to take countermeasures under certain circumstances prescribed by customary international law.[42] Countermeasures against the perpetrator State could be cyber in nature or taken through alternative means, but must always conform to the standards set forth by applicable international law, such as temporarily suspending certain bilateral treaty obligations during the period of the perpetrator State's non-performance of international obligations, provided that such measures are necessary to induce the perpetrator State to comply with the breached international obligation, are proportionate and do not themselves constitute a prohibited act under international law. Countermeasures in relation to cyber operations must not amount to a use of force or violate fundamental human rights, humanitarian obligations prohibiting reprisals or peremptory international legal norms (jus cogens). Countermeasures must be directed against the responsible, (i.e. perpetrator) State and must be proportionate to the injury suffered by the targeted State. Furthermore, they must be, as far as possible, reversible, intended to induce the perpetrator State to comply with its international obligations, and taken in such a way as to permit the resumption of performance of the obligations in question.

Furthermore, the injured (i.e. targeted) State must, in principle, first call upon the responsible State to fulfil its obligations and must notify it of its decision to take countermeasures. In certain circumstances and given the peculiarities of cyberspace, it may be necessary and justifiable to protect its rights for the injured State to take urgent countermeasures without warning the responsible State in advance of its intention to take countermeasures.

A cautious approach should be taken before adapting countermeasures responding to malicious cyber activities, particularly those involving non-State actor where, attribution remains uncertain.

[42] ICJ Nicaragua (1986), paras. 210, 248-249, 257-268; Gabčíkovo-Nagymaros Project (*Hungary v Slovakia*) [1997] ICJ Rep 7, paras. 83-88.

Necessity

A State may invoke necessity as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of that State if this was the only way for the State to safeguard an essential interest against a grave and imminent peril, whether cyber in nature or otherwise. A State may therefore launch a cyber activity in order to protect the electricity grid, food and water supply, rail traffic, distribution of social benefits, health of the population or in similar cases in which this would be indispensable for the functioning of the State and society.[43] In invoking necessity, however, a State may not seriously impair an essential interest of the affected State or States, or of the international community as a whole. Necessity may not be invoked by a State as a ground for precluding wrongfulness if the international obligation in question excludes the possibility of invoking necessity, or if the State has contributed to the situation of necessity.

E) Reparations

The State may invoke the international legal responsibility of the responsible State and demand satisfaction, the cessation of the internationally wrongful act and/or full reparation for the losses and damages incurred. Slovenia maintains that the rules and principles of State responsibility, as noted above, are applicable in the cyber context. Slovenia further considers that reparation may entail compensation for financially assessable damage, as well as assurances or guarantees of non-repetition.

F) Retorsions

International law does not preclude States from taking acts of retorsion –-unfriendly acts that are not inconsistent with their international obligations – including, for example, declaring diplomats from the perpetrator State *persona non grata*. Slovenia recognises that acts of retorsion must not deprive other States of their international rights. In light of the above, limiting the other State's access to servers or other digital infrastructure in Slovenian territory would constitute an act of retorsion. The European Union's Cyber Diplomacy Toolbox likewise offers measures that may be used to respond to malicious cyber activities which qualify as retorsion.

II. Peaceful settlement of disputes

Slovenia is of the view that States are obliged to seek the peaceful settlement of disputes to which they are parties, in accordance with Article 2(3) and Chapter VI of the UN Charter, including disputes related to State conduct in cyberspace. These means include negotiation, enquiry, mediation, conciliation, arbitration and judicial settlement.

[43] Tallinn Manual 2.0, Cambridge University Press 2017, Rule 26, para. 5.

Given the distinct nature and complexity of the disputes concerning cyber activities under international law, the establishment of specific expert bodies could be considered.

III. Individual criminal responsibility under international law

Under certain conditions, cyber activities may constitute international crimes resulting in individual criminal responsibility, as defined, for example, by the Rome Statute of the International Criminal Court (ICC) and customary international law. It should be stressed that the provisions are technology-neutral, as none of the crimes specified in the aforementioned instruments require any particular tool or means to be employed in order to constitute a crime, but instead focus on the effects of the perpetrated actions. It is therefore clear that international crimes can be committed through cyber activities.

However, particular challenges arise in determining the commission of such crimes through cyber activity, notably in the following four areas: (1) the seriousness of the crime, (2) jurisdiction of States, (3) attribution of criminal activity, and (4) establishing intent.

Cyber activity, whether an act of commission or an omission, should be considered an international crime if the nature, scale, effects and consequences meet the threshold of an international crime (*actus reus*), and if the mental element of intent or negligence is demonstrated (*mens rea*).

Given the inherently cross-border nature of cyber activities, determining State jurisdiction over such crimes may be significantly more challenging. A sufficient nexus must exist between the State and the cyber activity related to the crime in question.

Attribution of cyber activity to the persons alleged to have committed an international crime must be assessed in accordance with criminal law standards and must, therefore, meet the burden of proof required in criminal proceedings.

A similar standard should apply when determining the intent of persons conducting cyber activity in relation to an alleged international crime. A cautious approach is therefore advised, as criminal cases require high standard of proof.

Slovenia welcomes and further encourages the continued development of policy papers on prosecution of cyber-related crimes, such as the recent initiative undertaken by the Office of the Prosecutor of the ICC. [44]

CONCLUSION

As a staunch advocate of international law and the rule of law, Slovenia explains the importance of applicable international legal principles (the principles of sovereignty, non-interference and the prohibition of the threat or use of force), and particularly of international humanitarian law and human rights law in cyberspace as well. The

[44] Draft Policy on Cyber-enabled Crimes under the Rome Statute, 6 March 2025. Available at: https://www.icc-cpi.int/sites/default/files/2025-03/250306-OTP-Policy-on-Cyber-Enabled-Crimes-for-public-consultation.pdf.

International Law Commission's Articles on State Responsibility for Internationally Wrongful Acts are essential for establishing state responsibility for cyber activities, and the Rome Statute of the International Criminal Court is crucial for establishing individual criminal accountability for such activities. Slovenia believes that creating a new legally binding instrument is unnecessary. Nevertheless, Slovenia will promote and intensify discussions on this topic, both domestically and internationally.