Czech Republic

Position paper on the application of international law in cyberspace

Introduction

The rapid development of cyber capabilities and increasing number of harmful cyber activities have led States to address the question of how international law applies to cyberspace. The Czech Republic is aware of the opportunities and threats arising from the technological progress in information and communication technologies (ICTs) and fully endorses the international order based on international law that promotes an open, secure, stable, accessible and peaceful ICT environment and encourages responsible State behaviour in cyberspace. The Czech Republic considers international law to be a fundamental element of the framework for responsible State behaviour in cyberspace, which is essential to maintaining international peace and security, including in relation to cyber activities, and reaffirms that international law, including the United Nations Charter in its entirety, is applicable to State conduct in cyberspace and is essential to maintaining peace and stability in the ICT environment.[1] The Czech Republic supports the ongoing international efforts to determine how international law applies to cyberspace, including the work of the past and current UN Open Ending Working Group on security of and the use of information and communications technologies (OEWG) and the past UN Group of Govermental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (GGEs) and welcomes the growing number of national contributions of States on *how* international law applies in cyberspace. The Czech Republic is therefore pleased to contribute to these efforts, following several years of consultations between various governmental institutions, reflecting the views of a wide range of States and other stakeholders, including the International Committee of the Red Cross, and academic projects on the application of international law to cyber operations, such as the Tallinn Manual, the Oxford Process and the Cyber Law Toolkit. The Czech Republic believes that the expression of national positions on how international law applies to the States activities in cyberspace will enhance international dialogue and further development of a common understanding and consensus on lawful and acceptable State behaviour, and that such statements can help reduce the risk of misunderstanding and escalation between States arising from cyber activities.

In this position paper the Czech Republic sets out its current view on the application of certain provisions of international law in cyberspace. The position paper in no way aims to offer an exhaustive analysis, but is rather intended to express national position on certain relevant issues.

The position paper has been prepared in collaboration of the Ministry of Foreign Affairs of the Czech Republic, the Ministry of Defence of the Czech Republic, and the National Cyber and Information Security Agency and approved by the Committee for the Foreign Security Policy Coordination (CFSPC).

[1] See also the Progress Report of the 2022 OEWG, A/77/275, Annex, para 2; 2021 OEWG report, UN Doc A/75/816, Annex I, para 7; 2021 GGE report, UN Doc A/76/135, para 69, both later adopted by UNGA Resolution A/RES/76/19; 2015 GGE Report, UN Doc A/70/174, para 24, adopted by UNGA Resolution A/RES/70/237 and 2013 GGE Report, UN Doc A/68/98*, para 19, adopted by UNGA Resolution A/RES/68/243.

Table of content

Sovereignty

1. The principles of sovereignty and sovereign equality of States are fundamental concepts of international law, cornerstones of the UN Charter and apply in cyberspace, just as they do in other domains.[2]

2. The two facets of sovereignty are the internal facet, meaning that every State exercises its sovereignty over its territory, including the ICTs located therein, subject to its obligations under international law, including international human rights law, and the external facet, meaning that every State may freely and independently choose and develop its political, social, economic and cultural system and determine its foreign policy.

3. The sovereignty of every State must be respected. The principle of sovereignty forms a basis of various rules, such as the prohibition of intervention and the prohibition of the use of force. At the same time, sovereignty is a rule in its own right which is capable of being violated. Thus, cyber activities that do not amount to a prohibited intervention or a prohibited use of force may nevertheless amount to a violation of a State's sovereignty under international law. In such case, violation of one State's sovereignty by another State, including by a cyber means, would be considered an internationally wrongful act.[3]

4. On the other hand, the Czech Republic does not consider every cyber operation attributable to a State and having an effect in the territory or infrastructure of another State to be a violation of the latter's sovereignty. Cyberspace is a global and open domain and States often exercise their jurisdiction in another State's territory without legal repercussions. For instance, an organ of a State viewing a publicly available website hosted in another State for the purposes of obtaining information during a criminal investigation does not violate that State's sovereignty, despite exercising jurisdiction in its territory without its consent.[4]

5. Therefore, it is necessary to set a threshold where cyber activities could constitute a violation of the rule of sovereignty. The Czech Republic is of the view that cyber activities that rise above the level of negligible or *de minimis* effects and cause significant harmful effects on the territory of another State without the consent of that State could amount to a violation of the rule of sovereignty in relation to the State concerned. While there is no universal consensus on the threshold, the Czech Republic is of the opinion that the analysis should take into account the degree of infringement upon the target State's territorial integrity (i.e. the scope, scale, impact or severity of the effects of the operation and the causal link between the operation and its effects)

[2] As the *Island of Palmas (or Miangas) case (Neth. v. U.S.)*, 2 RIAA 829, ICGJ 392 (PCA 1928), 4th April 1928, Permanent Court of Arbitration [PCA] asserts: "[S]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."

[3] See Article 2, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries (ARSIWA), Yearbook of the International Law Commission, 2001 vol. II, Part Two.

[4] States party to the Convention on Cybercrime allow such operations in each other's territory. See Article 32 letter a) of the Convention on Cybercrime of the Council of Europe, adopted 23 November 2001, entered into force 1 July 2004, ETS 185.

or whether the operation interfered with or usurped inherently governmental functions.[5] In general, the impact or severity of cyber effects will be evaluated in the same manner and according to the same criteria as for physical activities. The Czech Republic will assess whether a violation of sovereignty has occurred on a case-by-case basis, since further State practice and opinio juris is needed to clarify the scope of customary law in this area over time.

6. The Czech Republic is of the opinion that the following cyber operations in one State's territory constitute violations of sovereignty, if attributed to another State, inter alia:

    a) a cyber operation causing death or injury to persons or significant physical damage;

    b) a cyber operation causing damage to or disruption of cyber or other infrastructure with a significant impact on national security, economy, public health, public safety or environment;[6] for instance, if such an operation causes a severe power outage affecting thousands of households;

    c) a cyber operation interfering with any data or services which are essential for the exercise of inherently governmental functions, and thereby significantly disrupting the exercise of those functions; for example, distributing ransomware which encrypts the computers used by a government and thus disables the payment of retirement pensions or other social benefits.[7]

Prohibition of Intervention

7. The obligation of non-intervention is a well-established customary rule of international law stemming from the principle of State sovereignty, which is also applicable to cyberspace. A definition of prohibited intervention was provided by the International Court of Justice in the 1986 *Nicaragua v United States case*: "A prohibited intervention must […] be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social, and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones."[8]

[5] See also Rule 4 para 15 of the Tallinn Manual 2.0 on the international law applicable to cyber operations, 2nd edition, CUP, 2017.

[6] Compare the UN GGE 2015 report, paragraph 13, letter f): "A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public[.]" and UN GGE report 2021 para. 42

[7] See also the *The Oxford Statement on Ransomware Operations*. Oxford Institute for Ethics, Law and Armed Conflict

[8] See para. 205 of *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986, ICJ Reports 1986 and UN General Assembly, *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, 24 October 1970, A/RES/2625(XXV).

8. The prohibition of intervention applies between States, and thus it is not applicable to the activities of individuals and non-State groups, unless their conduct can be attributed to a State under the rules of attribution under international law.[9] Cyber activities may constitute a prohibited intervention under international law if they are comparable in scale and effect to intervention in non-cyber contexts.

9. There are two conditions for a cyber activity to be considered as an intervention prohibited under international law:

    a) The activity has to tamper with the internal or external affairs of the State, also known as *domaine réservé*.[10] Internal affairs include, for instance, the conduct of elections; court proceedings; or the drafting and enactment of laws. External affairs include, for instance, the ratification and denunciation of treaties; consenting to official activities of other State's organs in its territory; or opening or closing down an embassy.

    b) The activity must be coercive in nature. Coercion is an activity intended to deprive, either directly or indirectly, the State of its ability to exercise control or govern matters within its internal and external affairs. The precise definition of coercion, and thus of unauthorised intervention, has not yet fully crystallised in customary international law, further State practice and opinio juris are therefore needed.

10. Furthermore, a causal nexus between the activity and the effect on the target State to change its behaviour has to be considered. The assessment whether a particular cyber activity has reached the threshold of prohibited intervention has to be done on a case-by-case basis.

11. There is a certain similarity between the terms "internal and external affairs" and "inherently governmental affairs", which is one of the defining elements of violation of sovereignty. The difference between actions that violate sovereignty and actions that violate the prohibition of intervention is that the latter is coercive, i.e., *intentionally* aims to influence the State's free will and choice.

12. The use of cyber means to target election systems to manipulate election results would, for example, constitute a violation of the obligation of non-intervention.[11]

13. Prohibition of intervention does not cover cyber activities broadly described as "propaganda", provided that they do not violate another specific rule of international law, such as direct and public incitement to commit genocide.[12] Mere influencing, criticism or persuasion do not meet the requirements to be qualified as prohibited intervention either.

---

[9] See para. 79 of Harriet Moynihan: *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention*, Chatham House, 2 December 2019.

[10] Such matters in which a State may decide freely include political, economic, social, and cultural system as well as formulation of foreign policy.

[11] See also *The Oxford Statement on International Law Protections Against Foreign Electoral Interference Through Digital Means*. Oxford Institute for Ethics, Law and Armed Conflict

[12] Article 3 of the UN General Assembly Convention on the Prevention and Punishment of the Crime of Genocide, 9 December 1948, United Nations

14. Therefore, assessed on a case-by-case approach and taking into account specific circumstances of the case, intervention in the internal or external affairs of the Czech Republic by cyber means may constitute a violation of the prohibition of intervention.

Due Diligence

15. Due diligence stems from a general international law principle that States must ensure that territory and objects over which they enjoy sovereignty are not used to harm the rights of other States. Due diligence entails 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."[13] Thus, in the cyber domain, due diligence requires States to take all reasonable and feasible measures concerning activities in cyberspace falling under their jurisdiction in order to prevent, eliminate or mitigate potentially significant harm to legally protected interests of another State.

16. There exist, to this day, divergent views on the precise normative character, scope, and content of due diligence in cyberspace. In the opinion of the Czech Republic, due diligence, under the conditions stated below, may be considered an obligation in its own right.

17. Due diligence equally applies in cyberspace as concluded by the UN GGE in 2015.[14] The Czech Republic is of the view that every State has an obligation to act against unlawful and harmful cyber activities emanating from or through its territory provided that it is aware of, or should reasonably be expected to be aware of, such activities. Due diligence applies in particular to activities of private individuals that violate the rights of other States, when harmful activities cannot be attributed to a particular State in accordance with the rules governing state responsibility or where only insufficient proof for such attribution exists.

18. The due diligence obligation is only triggered when the target State suffers serious adverse consequences. There is no universally accepted threshold of harm in international law and each case should be evaluated individually. The Czech Republic maintains that such harm does not need to be necessarily limited to physical damage to objects or physical injuries to persons by cyber means and could encompass other serious non-physical harm, resulting, for example, from the interference with or impairment of the use and operation of critical infrastructure. Such situations could also encompass, for example, malicious activities in cyberspace causing serious adverse consequences to medical and healthcare facilities in the Czech Republic.[15]

19. To ensure compliance with the due diligence obligation, States should take measures that may be reasonably expected, in the given context and circumstances, to act against harmful cyber activities that violate a right of another State. In procedural terms, due diligence might encompass a duty to inform and cooperate in the case of transboundary harm. At the same time, the means

[13] *Corfu Channel Case (United Kingdom v Albania)*; Merits, International Court of Justice (ICJ), 9 April 1949, Rep 4, p. 22.
[14] See para. 13 (c) of the UN GGE 2015 Report.
[15] See also *The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector*. Oxford Institute for Ethics, Law and Armed Conflict

to which a State has recourse in order to fulfil its due diligence obligation must be compatible with international law, including human rights obligations applicable to cyber activities. The Czech Republic understands due diligence as an obligation of conduct, not of result, therefore, as long as a State takes all reasonable measures, in accordance with the due diligence obligation, it cannot be held responsible if it is unable to prevent, mitigate or terminate wrongful cyber activities launched from or in transiting through its territory. Thus, the due diligence obligation does not require preventive monitoring of all activities in cyberspace. Moreover, factors such as technological and financial resources and overall material capabilities of the State, in the particular circumstances of each case, have to be taken into consideration when evaluating the compliance with the due diligence obligation.

20. In line with the above, the Czech Republic would consider a manifest violation of the due diligence obligation as an internationally wrongful act against which the Czech Republic, as the injured State, could take response pertaining to the law of State responsibility.

Peaceful Settlement of Disputes

21. The obligation of every State to settle their international disputes by peaceful means[16] remains one of the fundamental provisions of the UN Charter and general international law, which also applies in cyberspace.

22. In case of disputes that may endanger the maintenance of international peace and security, States shall seek solutions through negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice, as described in Article 33 (1) of the UN Charter.

23. The Czech Republic is of the view that the obligation to settle disputes peacefully does not preclude the right of States to take other measures in accordance with international law, including the UN Charter.

Use of Force

24. The prohibition of the threat or use of force by a State against the territorial integrity or political independence of another State or in any other manner inconsistent with the Purposes of the United Nations, as contained in Article 2(4) of the UN Charter, is one of the core provisions of the

[16] Article 2(3) and Article 33(1) of the *UN Charter*; Rule 65, p. 303 of the *Tallinn Manual 2.0 on the international law applicable to cyber operations*, 2nd edition, CUP, 2017.

UN Charter and a fundamental rule of customary international law,[17] which is also considered as peremptory norm of general international law (*jus cogens*).[18]

25. The prohibition of the threat or use of force contained in the UN Charter is deliberately general and encompasses any means and methods used (whether kinetic or cyber means).[19] Thus, the prohibition of the threat or use of force applies also in cyberspace.

26. Given the dependency of all States and societies on ICTs, cyber activities can have serious consequences not only in cyberspace but also in the physical world. Such activities can result in malfunction of critical infrastructure, physical damage or extensive economic loss, threaten national security or put human lives into jeopardy. The Czech Republic is of the opinion that cyber operation conducted in cyberspace could amount to the use of force under Article 2(4) of the UN Charter when the effects of the operation are comparable to those of a conventional character.

27. The UN Charter does not provide a definition of the term "*use of force*". Whether activities in cyberspace, attributable to a State under international law, violate the prohibition of the threat or use of force as contained in Article 2(4) of the UN Charter needs to be assessed on case-by-case basis. Activities conducted by cyber means that do not amount to a threat or use of force may still amount to a violation of sovereignty or a prohibited intervention into internal or external affairs. In the context of cyber operations, the Czech Republic is of the view that factors offered by the Tallinn Manual 2.0, such as severity, immediacy, directness, invasiveness, measurability of effects, military character, State involvement or presumptive legality of the cyber operation in question represent important criteria in the process of evaluation when deciding whether an act may be characterized as an unlawful use of force.[20]

28. Depending on the facts and circumstances, cyber operations attributable to a State and amounting to an unlawful use of force under Article 2(4) of the UN Charter may also constitute an "armed attack", under Article 51 of the UN Charter. The term "use of force" is generally perceived to be a broader concept than "armed attack", which is considered as the most grave form of the use of force.[21]

29. The UN Charter does not provide a definition of the term "armed attack", nor does it list the criteria for determining under what conditions an act amounts to an "armed attack". In accordance with the general guidance provided by the International Court of Justice there are two main factors to be considered when assessing whether a use of force constitutes an armed attack: the scale and

[17] See paras 188-190 of the *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment of 27 June 1986, ICJ Reports 1986.
[18] Article 53 and Article 64 of the *Vienna Convention on the Law of Treaties*, concluded 23 May 1969, entered into force 27 January 1980, 1155 UNTS 331.
[19] As stated by the International Court of Justice in the Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons, 8 July 1996, ICJ reports 1996, para 39: that Article 2 para 4 of the UN Charter (the prohibition of threat or use of force) "apply to any use of force, regardless the weapons employed. The Charter neither expressly prohibits, nor permits the use of any specific weapon."
[20] See p. 333 – 335 of the Tallinn Manual 2.0.
[21] See para 191 of the *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986, ICJ Reports 1986.

the effects of the particular act.[22] If a cyber operation was comparable in its scale and effect to an attack by conventional means (kinetic operations) in terms of its gravity, such as fatalities, damage and destruction, it could be considered as constituting an armed attack under Article 51 of the UN Charter.

30. The Czech Republic reiterates the provisions of the UN Charter and customary international law that if an armed attack occurs, the affected State may exercise its inherent right to individual or collective self-defence under Article 51 of the UN Charter. The exercise of the right to self-defence shall meet the conditions of necessity and proportionality,[23] but is not limited to cyber means and cyber domain, even if the armed attack was so conducted. Collective self-defence against a cyber operation amounting to an armed attack can be exercised only at the request of the victim State and within the scope of such a request.[24]

Law of Neutrality

31. The purpose of the law of neutrality is to spare neutral States[25] and their inhabitants from the effects of hostilities, and to prevent an escalation of an international armed conflict.

32. Due to worldwide interconnectivity of cyberspace, the law of neutrality is of great importance for cyber operations conducted as part of an international armed conflict. The Czech Republic shares the position taken by the Tallinn Manual 2.0 that the law of neutrality applies to cyber operations and cyber infrastructure.[26]

33. Cyber infrastructure located within the territory of a neutral State or under its exclusive control is protected by the State's territorial integrity and international humanitarian law. As long as such infrastructure is not used by the parties to the international armed conflict for the exercise of their belligerent rights, it is considered neutral in character irrespective of public or private ownership or the nationality of the owners. As such, it is protected from any harmful interference by the parties to the international armed conflict.

---

[22] See para 195 of the *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986, ICJ Reports 1986.

[23] See para 176 of the *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986, ICJ Reports 1986.

[24] See para 195 of the *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986, ICJ Reports 1986.

[25] For the purposes of this paper, the term "neutral State" refers to a State which is not a Party to an ongoing international armed conflict. See ICRC, *Commentary on the Third Geneva Convention*, Cambridge University Press, Cambridge, 2020 (forthcoming), para. 1082; San Remo Manual on International Law Applicable to Armed Conflicts at Sea (1994), para. 13(d); Manual on International Law Applicable to Air and Missile Warfare (2009), Rule 1(aa); Helsinki Principles on the Law of Maritime Neutrality (1998), Article 1.1; Tallinn Manual 2.0 (2017), Chapter 20, para. 2.

[26] Chapter 20 chapeau of the Tallinn Manual 2.0 on the international law applicable to cyber operations, 2nd edition, CUP, 2017.

34. Without prejudice to para 33 above, the Czech Republic takes the view that the use of a public, internationally and openly accessible network, such as the Internet, for military purposes, does not violate the law of neutrality even if it or its components are located on the territory of a neutral State, provided that doing so does not have any harmful effects on that State.[27]

35. A neutral State must remain impartial and may not knowingly engage in cyber activities that support the military action of one party to the international armed conflict. This means that a neutral State may not allow a party to the international armed conflict to use any cyber infrastructure located within its territory (as well as on vessels and aircrafts of the neutral State's nationality) for military purposes or to establish a new one for such purposes. In line with para 34 above this does not apply to the use of public, internationally and openly accessible networks such as the Internet without any effect on the neutral State.

36. A neutral State is also obliged to take all feasible measures to terminate an abuse of the cyber infrastructure located within its territory (as well as on the vessels and aircrafts of its nationality) by any party to the international armed conflict.

International Humanitarian Law (IHL)

37. IHL applies to cyber operations conducted in the context of both international and non-international armed conflicts. It protects persons who do not, or no longer, take part in the hostilities, and imposes limits on the the means and methods of warfare, conduct of hostilities, and provides for the protection of civilians and civilian objects during an ongoing armed conflict.

38. Principles and rules of IHL applicable in armed conflict govern all forms of warfare and all means or methods of warfare, including those of the future.[28] This is confirmed also by Article 36 of Additional Protocol I requiring States to review the lawfulness of such means and methods of warfare.[29] Thus, cyber operations conducted as a part of an armed conflict are governed by IHL in the same way as any other means or methods of warfare.

39. The Czech Republic endorses the view that a cyber operation during an armed conflict, which is attributable to a State or other party to the conflict under international law, may constitute an "attack" under IHL,[30] when the effects of such operation are comparable to those conducted by

[27] See also Rule 151 para 4 of the Tallinn Manual 2.0 on the international law applicable to cyber operations, 2nd edition, CUP, 2017.

[28] See para 86 of the International Court of Justice in the Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons, 8 July 1996, I.C.J. reports 1996.

[29] *"In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party."* Article 36 of the Additional Protocol I to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, of 8 June 1977.

[30] *„Attacks means acts of violence against the adversary, whether in offence or in defence*", Article 49 para 1 of the Additional Protocol I to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, of 8 June 1977.

conventional means or methods of warfare, for instance if a cyber operation is designed or reasonably expected to cause injury or death to persons or damage or destruction to objects during an armed conflict.[31]

40. Cyber operations conducted as part of hostilities during an armed conflict must always be conducted in compliance with all relevant IHL rules and in particular with IHL basic principles of humanity and military necessity,[32] distinction,[33] proportionality[34] and precaution.[35] Compliance with these principles in a cyber context may require specific considerations as the infrastructure in cyberspace is often used for both military and civilian purposes.

41. Parties to armed conflict must carefully design and use cyber tools to distinguish between the civilian population and combatants and between civilian objects and military objectives when conducting cyber operations. Civilians and civilian objects shall be protected from being the object of attack, including those carried out by cyber means.[36] Civilians are protected against attack unless and for such time as they are directly participating in hostilities. In case of doubt as to whether a person is a civilian, that person shall be presumed a civilian. Attacks shall be limited strictly to military objectives. In case of doubt as to whether cyber infrastructure that is normally used for civilian purposes is being used to effectively contribute to military action, it shall be presumed not to be so used. Foreseeable direct and indirect effects shall be taken into account when assessing the proportionality of an attack.

42. When conducting cyber operations, constant care must be taken to spare the civilian population, individual civilians and civilian objects,[37] for instance to ensure protection of essential civilian

[31] Rule 92, Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, 2nd edition, CUP, 2017, p. 415.

[32] "*The law of armed conflict is a compromise based on a balance between military necessity, on the one hand, and the requirements of humanity, on the other*." in Y. Sandoz, Ch. Swinarski and B. Zimmermann (eds), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, ICRC/Martinus Nijhoff Publishers, Geneva, 1987, p. 392–393 para. 1389

[33] Article 48 of the Additional Protocol I to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, of 8 June 1977.

[34] Article 51 para 5 letter b) and Article 57 of the Additional Protocol I to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, of 8 June 1977; „*Launching an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilians objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited*", Rule 14 of the ICRC Customary International Humanitarian Law Study, Vol. I, Rules, Henckaerts and Doswald-Beck, CUP, 2005.

[35] Articles 57–58 of the Additional Protocol I to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, of 8 June 1977; Rules 15–24 of the ICRC Customary International Humanitarian Law Study, Vol. I, Rules, Henckaerts and Doswald-Beck, CUP, 2005.

[36] *"The parties to the conflict must at all times distinguish between civilian objects and military objectives. Attacks may only be directed against military objectives. Attacks must not be directed against civilian objects."* (ICRC Study, rule 7); see also Article 52 para 1 of the Additional Protocol I to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, of 8 June 1977.

[37] Article 57 para 1 of the Additional Protocol I to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, of 8 June 1977.

infrastructure and services. All feasible precautions must be taken to protect civilians and civilian objects from adverse effects of attacks, including through cyber means.[38]

43. It is prohibited to make objects indispensable for the survival of the civilian population the object of attack, including through cyber means. It is likewise prohibited to destroy, remove or render them useless by cyber means.[39] Parties to an armed conflict must not disrupt the functioning of such objects, including through cyber means. All feasible measures must be taken to facilitate thier functioning and prevent harm to these objects, including by cyber operations.

44. Medical units, transport and personnel as well as impartial humanitarian personnel and objects shall not be the object of attack and they must be respected and protected at all times, including their cyber infrastructure.[40] All feasible measures must be taken to facilitate their functioning and to prevent harm to these facilities and persons.

45. Under all circumstances, parties to an armed conflict must not employ cyber tools that would spread or cause harm indiscriminately. Indiscriminate attacks, i.e., those that are of a nature to strike military objectives and civilians or civilian objects without distinction, are prohibited by IHL.[41]

46. Cyber operations that may be expected to cause incidental loss to civilian life, injury to civilians, or damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, are prohibited. In the cyber context, this would require parties to a conflict to assess the potential effects of cyber activities on both military and civilian infrastructure and users, including shared physical infrastructure that would affect civilians.

47. The Czech Republic emphasizes that the application of IHL to cyber activities in armed conflict by no means promotes the militarization of cyberspace, nor legitimizes cyber warfare, just as IHL does not legitimize any other form of warfare. On the contrary, it reduces the military use of cyberspace by creating limits and requiring for all used means and methods of warfare to be employed in accordance with its rules.

International Human Rights Law

48. With ongoing digitalization and technological advances of new technologies, the need to protect and respect all human rights in and with respect to cyberspace is becoming more urgent. While new technologies have great potential to contribute to the protection and promotion of human rights, they also pose significant challenges to human rights. The Czech Republic reiterates that

[38] *"The parties to the conflict must take all feasible precautions to protect the civilian population and civilian objects under their control against the effects of attacks."* (ICRC Study, rule 22); see also Additional Protocol I, Article 58.
[39] Article 54 para 1 of the Additional Protocol I to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, of 8 June 1977.
[40] See, e.g., Geneva Convention I, Article 19; Geneva Convention II, Article 12; Geneva Convention IV, Article 18; Additional Protocol I, Article 12; Additional Protocol II, Article 11; ICRC Study, rules 25, 28, and 29.
[41] Article 51 para 4 of the Additional Protocol I to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, of 8 June 1977.

the same rights that people have offline must also be protected online[42] and States must uphold their human rights obligations. Human rights instruments such as the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social and Cultural Rights (ICESCR), European Convention for the Protection of Human Rights and Fundamental Freedoms and other relevant human rights treaties and customary international law based on the Universal Declaration of Human Rights are applicable in cyberspace as they are in the physical domain. The Czech Republic further reiterates the universality, indivisibility, interdependence and interrelatedness of all human rights and fundamental freedoms.

49. Protection and promotion of human rights, both online and offline, is a longstanding priority for the Czech Republic. The Czech Republic promotes international collaboration to maintain a free, open, safe, secure and stable cyberspace where democracy, rule of law, and human rights and fundamental freedoms apply. In international organizations and other platforms, the Czech Republic promotes the human rights-based and human-centric approach to digital transition.

50. In the cyber domain, States must respect, protect and ensure human rights for all, including but not limited to the right to privacy, the right to freedom of thought, conscience and religion, the right to freedom of opinion and expression, including the right to seek, receive and impart information, the right to freedom of peaceful assembly and association, the right to equality and non-discrimination and the right to education, which are particularly relevant in the context of cyberspace and digital technologies. Implications of new and emerging technologies,[43] in particular data-driven technologies, must be taken into account especially in the context of the right to privacy, the right to freedom of opinion and expression and the right to freedom of peaceful assembly and association as stipulated in the ICCPR.[44]

51. In some situations, the obligations to respect and ensure human rights can be restricted. The Czech Republic recognizes that such restrictions must be provided by law, serve a legitimate purpose (such as protecting the rights of others, or national security), be necessary to achieve that purpose and be proportionate.[45]

State responsibility and Attribution

52. The customary international law on State responsibility, as reflected in the International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA), applies to State behaviour in cyberspace.

[42] Resolution of UN Human Rights Council, A/HRC/RES/38/7: The promotion, protection and enjoyment of human rights on the Internet (5 July 2018), operative para. 1.
[43] NATO, Emerging and disruptive technologies, 8 December 2022.
[44] UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999.
[45] UN Human Rights Committee, ICCPR General Comment No. 34 (12 September 2011), paras 21-36.; See also ICCPR General Comment No. 27 (1 November 1999), paras 14-16.

53. An internationally wrongful act is an act or omission that constitutes a breach of an international obligation of a State and is attributable to it under international law.[46]

54. The Czech Republic recognises the right of a State to attribute a cyber activity, either individually or collectively, in compliance with international law. A decision to attribute a cyber activity is a national prerogative and remains at the discretion of a sovereign State.

55. General international rules of attribution as reflected in ARSIWA are also applicable to cyberspace. A cyber operation is deemed an internationally wrongful act when it is attributable to a State under international law and constitutes a breach of an international obligation of the State. A cyber activity is attributable to a State if perpetrated by organs of States,[47] or persons or entities exercising elements of governmental authority and acting in that capacity in the particular instance,[48] or organs placed at the disposal of a State by another State.[49] Furthermore, States are responsible for international wrongful acts conducted by cyber means and perpetrated by non-state actors if such an actor in fact acts on the instruction of, or under the direction or control of that State in carrying out the conduct in question.[50]

56. Attribution is linked to the availability of information. It requires establishing the facts of the activity in question and the identity of the actors responsible for the purposes of attribution. Cooperation with relevant institutions to gather all available information, information sharing, consultations and coordination at national and international level can be required. Attribution is based not only on gathering relevant technical information but also on the assessment of a political and security context of a cyber activity, its nature, extent, and consequences. The ascertainment of the State of origin of a cyber activity is not in itself a determining factor and cannot stand as an argument alone.

57. Although States are not required to be absolutely certain to attribute a wrongful act, but rather to gather and reasonably assess the information available, a sufficient degree of certainty on attribution of a wrongful act to a particular State needs to be reached.

58. States are not obliged to disclose evidence in order to publicly attribute a cyber activity. The disclosure of evidence may be relevant when a legal proceeding is initiated (e.g., before the International Court of Justice).

Retorsion

59. Retorsion is a lawful, albeit unfriendly, act of an aggrieved State towards a wrongdoing State or an international organisation. Due to its lawfulness, retorsion is a readily available response to a harmful cyber activity that does not qualify as a breach of international law. However, it is also available in response to an internationally wrongful act. Response by retorsion can be combined

[46] See Article 2 ARSIWA.
[47] See Article 4 ARSIWA.
[48] See Article 5 ARSIWA.
[49] See Article 6 ARSIWA.
[50] See Article 8 ARSIWA.

with other types of response, such as countermeasures, if the legal conditions for such measures are met.

60. The Czech Republic is of the view that retorsion can be of both cyber and non-cyber nature. Examples include imposing *visa* restrictions, suspension of treaty negotiations, recalling a head of diplomatic mission, severance of diplomatic relations or economic measures such as import or export restrictions (unless the State has a specific obligation prohibiting it from doing so). Retorsion can be taken jointly by several States if none of the participating States has a legal obligation to refrain from that particular response.

Circumstances Precluding Wrongfulness

61. The Czech Republic recognises that wrongfulness of a cyber activity is precluded in the case of consent, self-defence, countermeasures in respect of internationally wrongful act, force majeure, distress or necessity.

62. Countermeasures are measures that are taken by an injured State against a State which is responsible for an internationally wrongful act, that would normally constitute a violation of an obligation under international law, but the wrongfulness of which is precluded as they are conducted in response to an ongoing internationally wrongful act committed by another State.[51] Conditions relating to resort to countermeasures are set forth by customary international law, as reflected in ARSIWA.

63. The Czech Republic recognises that the purpose of countermeasures is to induce the State that committed an internationally wrongful act to comply with its obligations under international law.[52] The ultimate goal of countermeasures is to attain the cessation of the violation of international law and reparation of the injury suffered. Other purposes, such as retribution or retaliation, do not constitute a ground for a lawful use of countermeasures.

64. The Czech Republic reserves its right to respond to cyber-related violations of international law obligations attributable to other States, in form of actions or omissions, by undertaking countermeasures, which can be carried out via both cyber and non-cyber means. States may respond with both traditional countermeasures, such as trade embargoes and financial sanctions, and cyber-enabled countermeasures, i.e., adverse cyber operations consisting in the non-performance for the time being of international obligations towards the responsible State.

65. Countermeasures shall be, as far as possible, reversible, shall not amount to the level of the threat or use of force and must be in compliance with other peremptory norms of international law, obligations for the protection of fundamental human rights, international humanitarian law prohibition on reprisals, applicable obligations under dispute settlement procedures and diplomatic and consular inviolability. They must be temporary and proportionate, i.e., commensurate with the injury suffered, taking into account the gravity of the internationally

[51] See Article 22 ARSIWA.
[52] See Article 49 para. 1 ARSIWA.

wrongful act and the rights of the injured State that were violated. In this context, the lack of physical damage shall not be considered as an impediment to undertaking justified countermeasures.

66. The Czech Republic recognises that an injured State is required to call upon the responsible State to fulfil its international obligations. Furthermore, prior to employing countermeasures, an injured State is required to notify the responsible State of its intention to take countermeasures and offer to negotiate with the responsible State. The Czech Republic, however, recognises that in case of urgency and in order to preserve rights of the injured State, countermeasures may be undertaken without such prior notification. In either way, given the specific nature of cyberspace that allows attackers to use various spoofing methods, the injured State may resort to countermeasures only if it is able to attribute the internationally wrongful act in question to the responsible State.

67. An injured State is not obliged to disclose evidence to justify resort to countermeasures but rather to be reasonable in its assessment and establish with sufficient certainty the attribution of an internationally wrongful act to a particular State. The Czech Republic recognises that an injured State is responsible for assessment of information in order to resort to countermeasures. Nevertheless, an injured State resorting to countermeasures may commit any international wrongful act if its assessment is carried out incorrectly.

68. The Czech Republic endorses that the State acts in conformity with international law under the principle of necessity when its action not in conformity with an international obligation is the only way for the State to safeguard an essential interest against a grave and imminent peril. This rule may be invoked only in exceptional cases, namely if there is no other real possibility of addressing the grave and imminent peril, such peril is clearly established on the basis of the evidence reasonably available at the time and provided the act would not result in serious impairment of an essential interests of another State or of the international community as a whole. The State may invoke necessity even if the total amount of potential damage has not yet been assessed, such damage also does not necessarily have to be physical.

Prague

February 2024