The Republic of Poland's position on the application of international law in cyberspace

I. Introduction

Changes brought about by the dynamic growth of digital technologies, including the implementation and development of e-government or the increasingly widespread electronic administration of critical infrastructure, result in countries' growing dependence on cyberspace[1]. On the one hand it offers new opportunities, but on the other hand it also poses challenges to state security and sovereignty.

The recent years have seen a series of actions in cyberspace, implemented by both state and non-state entities, that have targeted the stability and security of other nations and posed a challenge to assess their legality from the perspective of generally applicable norms of international law. Examples include the use of actions in cyberspace as part of the phenomenon commonly referred to as hybrid war, interference in democratic elections, and activities undertaken by terrorist groups.

Cyberspace poses a challenge to international law due to its partly non-territorial character, the speed with which actions can be carried out in it, and the relative anonymity it allows the users. Its specific nature requires explanation, sometimes also clarification, as to how norms of international law can be applied in the context of activities in cyberspace.

By presenting this position, the Republic of Poland wishes to join the states that have already formulated their views in this respect. In Poland's view, the practice of publicly presenting positions in key matters concerning international law increases the level of legal certainty and transparency, at the same time contributing to strengthening respect for international law commitments, and offers an opportunity to develop customary law.

Poland is also in favour of the discussion on how to apply international law to cyberspace, taking place in the UN in the field of information and telecommunications in the context of international security since 2013 within the Group of Governmental Experts, and also within the Open-Ended Working Group since 2021. As indicated in Poland's position presented at the UN in 2016, "Respect for international law and norms are a necessary condition for maintaining peace and security between States in cyberspace"[2].

Respect for the fundamental norms of international law is in turn instrumental in preventing international conflicts and their escalation. The above also applies to activities in cyberspace. This position is thus a natural continuation of Poland's two years of non-permanent membership of the Security Council (2018-2019), where the issue of respect for international law was one of Poland's priorities.

---

[1] Pursuant to the provisions of Polish law, cyberspace is the space for processing and exchanging information formed by ICT systems defined in Article 3(3) of the Act of 17 February 2005 on the computerisation of activities of entities performing public tasks (Journal of Laws of 2019, items 700, 730, 848 and 1590), including relations between them and relationships with the users – in accordance with Article 2(1b) of the Act of 29 August 2002 on the martial law and competences of the Supreme Commander of the Armed Forces and the rules of his subordination to the constitutional authorities of the Republic of Poland (Journal of Laws of 2017, item 1932).

[2] Report of the Secretary General: Developments in the field of information and telecommunications in the context of international security, 19 July 2016, A/71/172.

At the same time it should be noted that on 31 October 2019, a resolution of the Council of Ministers adopting the *Cybersecurity Strategy of the Republic of Poland for 2019–2024*[3] came into force. This document outlines the Polish government's strategic objectives as regards cyber security, that is increasing the level of resilience to cyber threats, and protection of information in the public, military, and private sectors. According to the Strategy, "The Republic of Poland – in cooperation with like-minded partners – shall promote the position that binding international law, most importantly the United Nations Charter, applies to cyberspace." One of the specific objectives listed in the Strategy is building a strong international position of the Republic of Poland in the area of cybersecurity. This position is in line with the objective.

It should also be noted that the EU Council conclusions *on the EU's Cybersecurity Strategy for the Digital Decade* of 9 March 2021 are applicable to cybersecurity. Before the issue was subject to a joint communication to the European Parliament and the Council, *The EU's Cybersecurity Strategy for the Digital Decade* of 16 December 2020 published by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy.

II. **Application of international law to actions in cyberspace**

1. The existing international law, including the Charter of the United Nations, applies to cyberspace. Therefore, states are required to adhere to international law in cyberspace.

The lack of universal treaties[4] referring directly to the actions of states and other actors in cyberspace does not mean that this space lies outside the law or is unregulated. The norms of international law derived both from the treaties and from other sources of law, in particular customary international law, apply to it. So far, the stance that the existing norms of international law apply to cyberspace has been taken among others by the European Union[5], the North Atlantic Treaty Organization[6], the UN Group of Governmental Experts (UN GGE)[7] and a number of states.

---

[3] Official Gazette of the Republic of Poland *Monitor Polski* of 2019, item 1037, http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20190001037.

[4] It should be noted, however, that the Council of Europe Convention on Cybercrime of 23 November 2001 is gradually gaining the status of a global treaty. 66 States, including 21 non-members of the Council of Europe, have become parties thereto.

[5] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7 February 2013, JOIN/2013/01 final; the Council Conclusions on malicious cyber activities, Brussels, 16 April 2018, 7925/18, stating among others that "the EU will continue strongly to uphold that existing international law is applicable to cyberspace and emphasises that respect for international law, in particular the UN Charter is essential to maintaining peace and stability. The EU underlines that States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to commit such acts (…)".

[6] Brussels Summit Declaration https://www.nato.int/cps/en/natohq/official_texts_156624.htm#20.

[7] https://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf

2. The principle of sovereignty applies to cyberspace

State sovereignty is a basic principle of international law.[8] According to this principle, states are independent and equal in international relations, while their territorial integrity and political independence are inviolable. As a consequence, states exercise supreme power over their own territory.[9]

The principle of sovereignty is closely linked to the principle of non-intervention in affairs falling under the domestic jurisdiction of a state. The norms concerning the jurisdiction of a state and the immunities of a state and its representatives are also derived from the principle of sovereignty.

A state exercises power over cyberspace users located within its territory, over IT infrastructure and over data. While respecting the norms of international law by which it is bound, it may exercise its sovereign prerogatives over such actors and facilities. It is also entitled to protect them. As a result, the Republic of Poland takes the position that the violation of a state's sovereignty may occur both in the event of an attack against state infrastructure and against private infrastructure. A mere fact that IT infrastructure is linked in a number of ways with an international network does not result in the state's losing any of its rights with respect to such infrastructure.

As it was indicated earlier, sovereignty has an external dimension as well. External sovereignty means that a state is independent in its external relations and is capable of freely engaging in any actions in cyberspace, also outside its own territory, subject to restrictions under international law. Another consequence of sovereignty is a state's capacity to enter into treaties, including those on cyberspace.

The principle of sovereignty requires other states to refrain from any actions that would violate sovereignty, and in particular states are obliged not to knowingly make their territory available for the purposes of acts that would violate the rights of other states.[9] Poland is of the opinion that in the event of a hostile operation conducted in cyberspace, causing serious adverse effects within the territory of a state, such actions should be considered a violation of the principle of sovereignty, irrespective of whether such effects are of kinetic nature or are limited to cyberspace. The violation of the principle of sovereignty may be exemplified by a conduct attributable to a third country that consists in interfering with the functioning of state organs, for instance by preventing the proper functioning of ICT networks, services or systems of public entities, or by a theft, erasure or public disclosure of data belonging to such entities.

---

[8] See the International Court of Justice's judgment in the case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), ICJ. Rep. 1986, § 263.

[9] "Sovereignty 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", an arbitral award in the Island of Palmas case (United States v. Netherlands, 1928); the judgment of the International Court of Justice in the Corfu Channel case (United Kingdom v. Albania), ICJ. Rep. 1949, p. 19; see "Between independent States, respect for territorial sovereignty is an essential foundation of international relations", the judgment of the International Court of Justice in the Corfu Channel case (United Kingdom v. Albania), ICJ. Rep. 1949, p. 35; the International Court of Justice's judgment in the case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), ICJ. Rep. 1986, § 251.

States should exercise due care to ensure that the IT infrastructure located within their territory is not used for unauthorised actions targeted at third countries. The same applies to persons staying within the territory of the state. An assessment of whether the state exercised due care or not should be contingent upon its technological advancement, expertise/resources and knowledge about actions in cyberspace initiated within its territory.

Actions in cyberspace that violate the prohibition of the use of force and the principle of non-intervention in affairs falling under the domestic jurisdiction of a state would also violate the principle of sovereignty.

3. Actions in cyberspace may constitute unlawful intervention in affairs falling under the domestic jurisdiction of a state

Intervention in internal or external affairs of another state that fall under its domestic jurisdiction is an action that contravenes international law.[10] The principle of non-intervention is a natural consequence of the principle of sovereignty – to the extent to which the state exercises its exclusive sovereign rights, the other states have an obligation to respect them.

The threshold for considering a specific operation in cyberspace to be in breach of the principle of non-intervention is higher than in the case of deeming it solely a violation of the principle of sovereignty. To be in breach of international law, an intervention must include the element of coercion that aims at influencing the state's decisions belonging to its *domaine réservé*, i.e. the area of state activity that remains its exclusive competence under the principle of sovereignty.[11] Therefore, it is possible to refer to a violation of the non-intervention principle if a state interferes with internal or external affairs falling under the exclusive competence of another state by using an element of coercion.

There is no universally acceptable definition of "coercion", but an unambiguous example of a prohibited intervention is the use of force.

A cyber operation that adversely affects the functioning and security of the political, economic, military or social system of a state, potentially leading to the state's conduct that would not occur otherwise, may be considered a prohibited intervention. In particular, any action in cyberspace that would prevent the filing of tax returns online or any interference with ICT systems that would prevent a reliable and timely conduct of democratic elections would be a violation of international law. Similarly, depriving the parliament working remotely of the possibility of voting online to adopt a law or modifying the outcome of such voting would also be such a violation. It should also be noted that a wide-scale and targeted disinformation campaign may also contravene the principle of non-intervention, in particular when it results in civil unrest that requires specific responses on the part of the state.

[10] The principle of non-intervention is referred to in Article 2(7) of the Charter of the United Nations (with respect to the relations between the UN and States) and the Declaration on Principles of International Law adopted by UN General Assembly Resolution No 2625 of 24 October 1970 (with respect to international relations).

[11] The International Court of Justice's judgment in the case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), ICJ. Rep. 1986, § 205.

4. In certain circumstances actions in cyberspace may constitute a violation of the prohibition of the use of force

The prohibition on the threat or use of force is laid down in Article 2(4) of the Charter of the United Nations[12] and customary international law. According to the Advisory Opinion of the International Court of Justice on the legality of the threat or use of nuclear weapons[13], an action may be considered the use of force irrespective of the means used. What matters are the effects of the actions taken. As a result, it cannot be ruled out that in some circumstances a cyberattack will reach such a threshold that it will be deemed the use of force. Perceiving a cyberattack as the use of force is supported by the possibility of it causing similar effects to those caused by a classic armed attack executed with the use of conventional weapons. When assessing whether or not a cyber operation reaches the threshold of the use of force, the situation must be analysed individually, taking into consideration the circumstances of actions taken in accordance with the requirements of international law. An action in cyberspace that leads to: a permanent and significant damage of a power plant, a missile defence system deactivation or taking control over an aircraft or a passenger ship and causing an accident with significant effects may be considered the use of force. This list is not exhaustive – the legal qualification will always depend on the circumstances of a specific attack.

A cyberattack that does not reach the threshold of the prohibited use of force may be deemed a prohibited intervention or an action that violates the principle of sovereignty.

5. A cyberattack may be qualified as an armed attack. The right to self-defence applies to cyberspace

Pursuant to Article 51 of the Charter of the United Nations and customary international law, a state has the right of self-defence in the event of an armed attack. In the context of cyberspace, a cyberattack that results in death or injury of people or damage or destruction of property of significant value may be considered an armed attack. In such circumstances, according to international law, a state enjoys the right of self-defence, however, this right should be exercised in line with the principles arising from customary international law, namely the principle of necessity and proportionality.[14]

Self-defence does not need to involve the same means through which the armed attack was inflicted. In response to a cyberattack that reaches the threshold of an armed attack, it is possible to respond both in cyberspace exclusively or with the use of traditional armed forces. Deprivation of the right to respond to such a cyberattack with kinetic means could render the self-defence right illusory when the perpetrator of an armed attack is little dependent on its functioning in cyberspace.

---

[12] Article 2(4) of the Charter of the United Nations: *"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."*

[13] Advisory Opinion of the International Court of Justice on the Legality of the Threat or Use of Nuclear Weapons, ICJ Rep. 1996, § 39.

[14] Advisory Opinion of the International Court of Justice on the Legality of the Threat or Use of Nuclear Weapons, ICJ Rep. 1996, § 41.

According to international law, the right of self-defence may also apply to cyberattacks reaching the threshold of an armed attack inflicted by non-state actors. The right of collective self-defence applies to cyberspace as well. This is supported by a declaration adopted by the representatives of states attending the meeting of the North Atlantic Council during the summit of the North Atlantic Treaty Organization in Wales in 2014. The declaration stipulates among others that a cyberattack can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Its impact could be as harmful to modern societies as a conventional attack. It was, therefore, affirmed that cyber defence is part of NATO's core task of collective defence.[15]

6. A state is responsible for actions in cyberspace that violate international law

Norms of customary international law concerning the assignment of responsibility to a state are reflected to a large extent in the articles covering the states' responsibility for internationally wrongful acts as adopted in 2001 by the International Law Commission[16] (hereinafter referred to as "Articles on the Responsibility of States").

The document reiterates that "Every internationally wrongful act of a State entails the international responsibility of that State." (Article 1). A state is responsible for conduct consisting of both an action or omission that is attributable to the state under international law and constitutes a breach of an international obligation of the state (Article 2). Articles 4–11 describe the rules governing the attribution of responsibility to a state. According to these rules, the State is responsible among others for the conduct of its organs, persons or entities which, even though they are not organs, are empowered by law to exercise governmental authority, as well as persons or groups of persons acting on the instructions of, or under the direction or control of that state.

The above norms also apply to conduct of states in cyberspace. The state may therefore be responsible for internationally wrongful acts of, for instance of hacker groups or individual hackers, if the conditions expressed in the Articles on the Responsibility of States are satisfied. At the same time, it should be remembered that the specific nature of cyberspace severely hampers the attribution of internationally wrongful acts to states or other actors.

7. International human rights law applies to cyberspace

High anonymity, control of data flow, and a largely non-territorial nature of cyberspace pose a challenge for protecting human rights online. Nonetheless, international human rights law applies to conduct in cyberspace. Rights that people have offline must also be protected online.[17] States have an obligation not to violate human rights and to protect such rights when they are violated by non-state actors or other states. The above-mentioned examples of

[15] Declaration of the NATO Summit in Wales, 2014, paragraph 72.
[16] The text annexed to UN General Assembly Resolution No. 56/83 of 12 December 2001.
[17] UN Human Rights Council Resolution "The promotion, protection and enjoyment of human rights on the Internet" of 29 June 2012.

unlawful actions by external actors that constitute violations of a state's sovereignty or an act of violence may at the same time result in a violation of human rights.

Freedom of speech and right to privacy require special protection in cyberspace. As the European Court of Human Rights pointed out, "the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general".[18] Depriving individuals of access to the Internet or specific websites may constitute a violation because, as the Court emphasised, "user-generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression".[19] At the same time, it must be taken into account that such rights may be subject to restrictions necessary in a democratic society, in particular due to public security interest, protection of public order, health and morality or the protection of rights and freedoms of other persons.

Protection of international human rights law in the context of cyberspace requires efforts for the open and safe Internet. Respecting sovereignty in cyberspace must not serve as an excuse for violations of international human rights law. The effective protection of human rights requires that a state refrain from unjustified interference with rights and freedoms exercised on the Internet, and in some circumstances it requires positive actions aimed at guaranteeing effective execution and protection of human rights on the Internet.

8. The norms of international humanitarian law apply to cyberspace

The norms of international humanitarian law (IHL)[20] apply in the event of an armed conflict, an international or non-international one. The basic principles of international humanitarian law include the principle of humanity, proportionality, military necessity and distinction. The requirements of international humanitarian law apply also to actions carried out in cyberspace during an armed conflict. When taking actions in cyberspace, it is necessary to consider both direct and indirect effects of such operations.

9. Retorsion and countermeasures as a response to harmful actions in cyberspace

In accordance with international law, a state has a right to take measures in response to hostile actions in cyberspace that do not reach the threshold of an armed attack[21].

International practice shows that states may use a range of measures to ensure that law is respected by other actors subject to international law. In particular the state which is

[18] Times Newspapers Ltd v. the United Kingdom (No. 1 and 2), applications nos. 3002/03 and 23676/03, ECHR judgment of 10 March 2009[1.]

[19] Cengiz and Others v. Turkey, application no. 48226/10 and 14027/11, ECHR judgment of 1 December 2015, § 52.

[20] These are expressed in particular in four Geneva Conventions of 1949 and two Additional Protocols of 1977 and in customary international law.

[21] It is illustrated by Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, which "establishes a framework for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States" (recital 7).

the target of an cyberattack may respond to hostile actions by using retorsion or countermeasures.

Retorsion is a response of the state to actions contrary to its interest or hostile actions of another state. Measures taken as a retorsion may be in reaction to both legal and illegal actions of another subject of international law, but in itself they must be in compliance with international law.

Countermeasures are the reaction of a state whose international rights have been violated by another actor. They consist in refraining from the performance of international obligations for some time in order to persuade the state that violates international law to fulfil its obligations and to persuade it against further violations.

At the same time, the Republic of Poland expresses the view that the evolution of customary international law over the last two decades provides grounds for recognising that a state may take countermeasures in pursuit of general interest as well. In particular, the possibility of taking such measures materialise itself in response to states' violations of peremptory norms, such as the prohibition of aggression.

When applying such measures, the state is required to act in accordance with the principle of proportionality. Moreover, both retorsion and countermeasures cannot constitute the violation of norms pertaining to fundamental human rights, obligations under international humanitarian law and peremptory norms.