International law and cyberspace

Finland's national positions

Introduction

In line with its general support to rules-based international cooperation and respect for international law, Finland sees international law as an essential framework for responsible State behaviour in cyberspace. In the same vein, the UN Group of Governmental Experts (GGE) has reaffirmed that "international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment". [1] As this formulation, reflecting the specific mandate of the GGE, focuses on questions of international peace and security, there is reason to underline that the same applies to other rights and obligations of States, whether based on treaty law or customary international law.

While the existing rules and principles of international law are applicable in cyberspace, the application of certain provisions may give rise to practical problems due to the specific characteristics of cyberspace. Finland therefore welcomes the current exchange of views on particular questions regarding how international law applies to State use of information and communication technologies and wishes to contribute to the discussion by commenting on some of the issues that have been raised recently in this regard.

Sovereignty

It is undisputed that the principle of State sovereignty applies in cyberspace. While cyberspace as a whole cannot be subject to appropriation by any State, each State has jurisdiction over the cyber infrastructure and the persons engaged in cyber activities within its territory.[2] Sovereignty confers each State the exclusive right to exercise the functions of a State within a certain territory,[3] and protects its territorial integrity and political independence from interference by other States.[4] In this sense, sovereignty is a foundational principle of the international legal order.

---

[1] See Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013 Report (UN Doc. A/68/98, para.20; 2015 report (UN Doc. A/70/174), para. 24.

[2] The Group of Governmental Experts has stated in this regard that "State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related and to their jurisdiction over ICT infrastructure within their territory". See GGE 2015 Report, para. 27. Other bases of jurisdiction may be applicable to cyber activities in accordance with international law.

[3] As Judge Max Huber stated in the *Island of Palmas* arbitral award: "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." See *Island of Palmas (Netherlands v. the US),* 2 UNRIAA 829, 838 (PCA 1928).

[4] According to the International Court of Justice, "between independent States, respect for territorial sovereignty is an essential foundation of international relations." See *Corfu Channel Case (UK v. Albania)*, ICJ reports 1949, p. 4, at 35.

The principle of State sovereignty has also given rise to a number of specific rules, such as those prohibiting the use of force and intervention in the internal affairs of other States. Below the threshold of prohibited intervention, all States have an obligation to refrain from acts that violate the territorial integrity or political independence of other States.

The International Court of Justice has consistently confirmed that it is a duty of every State to respect the territorial sovereignty of others. This applies to unauthorized intrusions to physical spaces such as overflight of a State's territory by an aircraft belonging to another State or under its control,[5] penetration of territorial waters by foreign warships,[6] conducting of certain activities in another State's territory without its consent[7] but also to producing effects in another State's territory without physical intrusion.[8] According to the Court, it is "quite obvious that a State possesses a legal interest in the protection of its territory from **any form** of external harmful action".[9]

Similarly, a non-consensual intrusion in the computer networks and systems that rely on the cyber infrastructure in another State's territory may amount to a violation of that State's sovereignty. The prohibition of cyber operations violating the territorial sovereignty of another State protects, first of all, the cyber infrastructure located in the territory of that State, or otherwise under its jurisdiction, as well as computer networks and systems supported by such infrastructure, from material harm. The situation is the same irrespective of whether such infrastructure belongs to or is operated by governmental institutions, private entities or private individuals. In addition to material harm that may be caused by such an operation, other relevant considerations include whether an intrusion in the cyber infrastructure triggers a loss of functionality of the equipment relying on it, or modifies or deletes information belonging to the target State, or to private actors in its territory.

More generally, an unauthorized intrusion by cyber means may be seen as a violation of the target State's territorial sovereignty if it interferes with data or services that are necessary for the exercise of inherently governmental functions. This rule put forward in the Tallinn Manual 2.0 [10] is consistent with the understanding of violations of sovereignty as unauthorized exercise of authority in another State's territory. Finally, cyber operations against objects that enjoy sovereign immunity (warships, ships owned by a State and used only for government or non-commercial service; State aircraft) can be characterized as violations of sovereignty.[11]

---

[5] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),* Merits, Judgment, I.C.J. Reports 1986, p. 14, paras. 251, 253, 292.

[6] *Corfu Channel case (United Kingdom v. Albania), Judgment, I.C.J. Reports 1949, p. 4,* at 26, 35, 36.

[7] *Certain Activities carried out by Nicaragua in the Border Area (Costa Rica v,. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica)*, Judgment, I.C.J. Reports 2015, p.665, paras. 66,67,69, 93, 221-223 and 229.

[8] *Nuclear Tests (Australia v. France)*, Judgment, I.C.J. Reports 1974, p. 253, para. 454.

[9] *Ibid*. para 456, emphasis added.

[10] Michael N. Schmitt (ed.), *Tallinn Manual 2.0*, Cambridge University Press 2017, Rule 4, para. 15.

[11] Cf. *Ibid*., Rule 5.

The argument has been raised recently that no legal consequences could be attached to sovereignty as a general principle, at least for the purposes of cyber activities. It is not only difficult to reconcile such an idea with the established status of the rule prohibiting violations of sovereignty in international law but it also gives rise to policy concerns. Agreeing that a hostile cyber operation below the threshold of prohibited intervention cannot amount to an internationally wrongful act would leave such operations unregulated and deprive the target State of an important opportunity to claim its rights.

Finland sees sovereignty as a primary rule of international law, a breach of which amounts to an internationally wrongful act and triggers State responsibility. This rule is fully applicable in cyberspace. Whether an unauthorized cyber intrusion violates the target State's sovereignty depends on its nature and consequences and is subject to a case-by-case assessment.

Illegal intervention

A hostile interference by cyber means may also breach the customary prohibition of intervention in the internal affairs of another State, provided that it is done with the purpose of compelling or coercing that State in relation to affairs regarding which it has free choice (so-called *domaine réservé*). The requirement of coercion leaves out lesser forms of influence and persuasion that are commonplace in international relations. The limitation to sovereign affairs – such as a State's political, economic or cultural system or the direction of its foreign policy[12] – further distinguishes prohibited intervention from measures, the purpose of which is to compel another State to comply with its international obligations.

For a cyber operation to amount to a prohibited intervention, both above-mentioned elements must be present. Most open questions relate to the element of coercion and to how it manifests itself in cyber operations. For instance, while the conduct of elections belongs undisputedly to the internal affairs of each State, all methods of electoral interference do not display the element of coercion.[13] Hacking of voter databases or manipulation of vote counts in order to alter the election results has nevertheless been recognized as a fairly clear case. To be comparable to a real world intervention, cyber interference must also be of a serious nature.

According to the International Court of Justice, the element of coercion is particularly clear if force is used through means of military action, threats of such action, or through support to armed groups in another State. [14] Military or economic pressure may also qualify as coercion. Hostile cyber interference done with the purpose of promoting or supporting armed action in another State could constitute an example of prohibited intervention, provided that it seeks to force a certain policy change.[15]

[12] *Military and Paramilitary Activities in and against Nicaragua,* para. 205.
[13] All methods of electoral interference are not coercive, see EU vs. disinfo, 10 *Methods of electoral interference* (2019).
[14] *Military and Paramilitary Activities in and against Nicaragua*, para.247.
[15] *Ibid.*, see also paras 241 and 242. See also Friendly Relations Declaration, UN Doc. A/RES/2625(XXV).

Compared to a violation of sovereignty, the requirement of coercive nature and that of *domaine réservé* make the threshold of prohibited intervention considerably higher. This underlines the importance of continued understanding of sovereignty as not only a principle but also an independent primary rule of international law.

Transboundary harm

Another cardinal principle flowing from sovereignty, closely related to the obligation to respect the sovereignty of other States, is each State's obligation not to knowingly allow its territory to be used to cause significant harm to the rights of other States. It is widely recognized that this principle, often referred to as due diligence, is applicable to any activity which involves the risk of causing significant transboundary harm.[16] Due diligence is a variable standard in the sense that its content can change over time as a result of technological development or changes in risk assessment,[17] and as such fully applicable to cyber operations.

States may thus not knowingly allow their territory, or cyber infrastructure within a territory under their control, to be used to cyber operations that produce serious adverse consequences for other States. While only States can violate sovereignty, the sovereignty-based obligation of due diligence extends to private activities taking place in a State's territory. Significant harm caused to other States by private cyber activities may give rise to a State's international responsibility but only if the State in question has breached its due diligence obligations.

Some legal obligations are inherent in the principle of due diligence and apply to cyber activities even in the absence of cyber-specific elaborations of the principle. For instance, if a State knows about a planned cyber activity in its territory likely to affect another State adversely and seriously, it must notify that other State. In addition to actual knowledge of harmful acts emanating from the territory of a State, a State's responsibility may be engaged in situations in which it should have known about the activities in question. It is nevertheless clear that "it cannot be concluded from the mere fact of the control exercised […] over its territory […] that [a] State necessarily knew, or ought to have known, of any unlawful act perpetrated therein".[18]

If harmful cyber activity takes place and causes serious harm to another State, the State of origin must take appropriate action to terminate it, as well as to investigate the incident and bring those responsible to justice. In order to be able to do this, States should have the necessary procedural

[16] International Law Commission, Draft Articles on the *Prevention of transboundary harm from hazardous activities*, art. 3: "The State of origin shall take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof", *Yearbook…* 2001, vol. II (Part Two), pp. 144–170; International Law Association, Second Report on Due Diligence in International Law, July 2016, p. 6: "This broad principle of due diligence can be understood as underlying more specific rules of due diligence. Hence, it can be viewed as a default standard that is triggered in operation if no more specific elaboration of due diligence or stricter standard is in existence."

[17] International Tribunal for the Law of the Sea, Seabed Disputes Chamber, *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, Advisory opinion, 1 February 2011, List of Cases: No. 17, para. 117.

[18] International Court of Justice, *Corfu Channel case*, Judgment of April 9th, 1949, I.C.J. Reports 1949, p.4, at 18.

and legal mechanisms in place. It should nevertheless be recalled that due diligence is an obligation of conduct, not one of result. In general, what is required of States is that they take all measures that are feasible under the circumstances. A particular question in this regard is related to the position of transit States through which a particular harmful data is routed. Much depends on whether such a State has any knowledge of the ongoing operation, or ability to take feasible measures to terminate it.

Furthermore, while States must show due diligence in the control of the national territory, doing so does not release them from the observance of other international obligations such as those related to human rights.

State responsibility

The law of State responsibility consists of secondary rules that apply generally in the absence of clear specific rules that modify their effect. As there is no specific regulation concerning State activities in cyberspace that would constitute such *lex specialis*, it can be concluded that the normal rules of State responsibility apply in cyberspace.

When a State's cyber operation violates its obligations under international law, it constitutes an internationally wrongful act. An internationally wrongful act of a State entails its international responsibility and gives rise to an obligation to make full reparation for the damage that may be caused by the act.[19] This requires that the act is attributable to the State. The rules of attribution reflected in the UN International Law Commission's Articles on State Responsibility[20] remain fully valid in cyberspace. If State organs, or private groups or individuals acting on behalf of the State, can be identified as the authors of a cyber operation that violates the State's international obligations, its international responsibility is engaged. It is in this regard useful to distinguish identification as a technical operation from attribution as a legal operation. Identification may be technically challenging given the often covert nature of hostile cyber activities but this is without consequence to the legal rules of attribution.

An internationally wrongful act may justify recourse to countermeasures by the injured State if the State responsible for an internationally wrongful act declines to cease the wrongful conduct or pay reparation. Countermeasures may only be taken with the purpose of ensuring compliance, not for retaliation. Countermeasures may furthermore not breach the prohibition of the threat or use of force, or other peremptory norms of general international law, and must be consistent with other customary law requirements and limitations concerning countermeasures, most of which are reflected in the International Law Commission's Articles on State Responsibility.[21] Some of the procedural requirements concerning countermeasures may nevertheless require

[19] International Law Commission, *Responsibility of States for Internationally Wrongful Acts* (2001), available at www.legal.un.org/ILC (ARSIWA) .
[20] *Ibid.*, arts. 4–11.
[21] *Ibid*., arts. 49–54.

adjustment. For instance, it may be possible to attribute a hostile cyber operation only afterwards whereas countermeasures normally should be taken while the wrongful act is ongoing.

There is no general obligation for a State taking countermeasures to disclose the information on the basis of which the action is taken. At the same time, it is in each State's best interests to ensure that a decision to take countermeasures is based on solid evidence, given that recourse to countermeasures would otherwise constitute an internationally wrongful act. A State that responds to a hostile cyber operation must therefore have adequate proof of the source of the operation and convincing evidence of the responsibility of a particular State.

Public attribution, as a sovereign choice, is primarily a question of political consideration. Public attribution may nevertheless have legal effects to the extent it includes determinations of conduct that constitutes an internationally wrongful act.

In addition to countermeasures, other circumstances precluding wrongfulness may justify taking of cyber measures that would otherwise constitute an internationally wrongful act.[22] This may be the case, for instance, if deviating from an international obligation is the only way for the State to safeguard an essential interest against a grave and imminent peril. Facing such an exceptional situation, a State may deviate from its international obligations within the limits specified in the law of State responsibility.[23]

Use of force/ armed attack

While there is currently no established definition of a cyberattack that would pass the threshold of "use of force" in the sense of article 2(4) of the UN Charter, or "armed attack" in the sense of article 51, it is widely recognized that such a qualification depends on the consequences of a cyberattack. For a cyberattack to be comparable to use of force, it must be sufficiently serious and have impacts in the territory of the target State, or in areas within its jurisdiction, that are similar to those of the use of force. A threat of such a cyberattack could also violate Article 2(4) of the Charter, if the threat is sufficiently precise and directed against another State.

Similarly, most commentators agree that when the scale and effects of a cyberattack correspond to those of an armed attack responding to the cyberattack is justifiable as self-defence. It is obvious that the attack must have caused death, injury or substantial material damage, but it is impossible to set a precise quantitative threshold for the effects, and other circumstantial factors must be taken into account in the analysis, as well. A widely discussed question is, to what extent the definition of a cyberattack comparable to an armed attack should take account of the indirect and long-term impacts of the attack. In any case, this would require that the impacts can be assessed with sufficient precision. A question has also been raised, whether a cyberattack producing significant economic effects such as the collapse of a State's financial system or parts of its economy should be equated to an armed attack. This question merits further consideration.

[22] ARSIWA, Chapter V, Circumstances precluding wrongfulness.
[23] Ibid., art. 25. See also Tallinn Manual 2.0, Rule 26.

Any interpretation of the use of force in cyberspace should respect the UN Charter and not just the letter of the Charter but also its object and purpose, which is to prevent the escalation of armed activities. This would mean, for instance, that the distinction between armed attack as a particularly serious violation of the Charter, on the one hand, and any lesser uses of force, on the other, is preserved. Similarly, the conditions for the exercise of the right of self-defence apply in cyberspace as they do with regard to the use of armed force. The right of self-defence arises if a cyberattack comparable to an armed attack occurs and can be attributed to a particular State.[24] It is reasonable to think that a State victim to such an attack can respond with either cyber means or armed action. At the same time, the use of force must not be disproportionate or excessive.

International Humanitarian Law

International humanitarian law only applies to cyber operations when such operations are part of, or amount to, an armed conflict. Most so far known cyberattacks have not been launched in the context of an armed conflict or met the threshold of armed conflict. At the same time, when cyber means are used in the context of a pre-existing armed conflict, as has been done in many current conflicts, there is no reason to deny the need for the protections that international humanitarian law provides.

This includes that cyber means and methods of warfare must be used consistently with the principles of distinction, proportionality and precautions, as well as the specific rules flowing from these principles. When assessing the capacity of cyber means and methods to cause prohibited harm, their foreseeable direct and indirect effects shall be taken into account. Constant care shall be taken to ensure the protection of civilians and civilian objects, including essential civilian infrastructure, civilian services and civilian data.

The unique characteristics of cyberspace, such as interconnectedness and anonymity, may affect how international humanitarian law is interpreted and applied with regard to certain cyber means and methods warfare. The related problems can nevertheless mostly be solved on the basis of existing rules. New technologies do not render the existing rules of international humanitarian law meaningless or necessarily require new legal regulation. Furthermore, while international humanitarian law is *lex specialis* in an armed conflict, it does not override other areas of international law, such as human rights law, which may continue to apply throughout the conflict.

Human rights law

A number of specific human rights such as the freedom of opinion and expression, including the right to access to information, and the right to privacy are particularly relevant in cyberspace. It should nevertheless be underlined that individuals enjoy the same international human rights

[24] While the possibility of a cyberattack rising to the level of an armed attack without the involvement of any State is conceivable, the related questions of self-defence against non-State actors are too complicated to be discussed here.

with respect to cyber-related activities as otherwise and, accordingly, that States are bound by all their human rights obligations both online and offline. Furthermore, each State has to protect individuals within its territory and subject to its jurisdiction from interference with their rights by third parties.