Government Offices of Sweden

July 2022

Position Paper on the Application of International Law in Cyberspace

Introduction

The applicability of existing international law, including the UN Charter, in cyberspace has been confirmed by the United Nations Group of Governmental Experts (UN GGE) and by the United Nations Open-ended Working Group (OEWG).[1] The Reports of both groups have been adopted by the UN General Assembly.[2] UN Members have thus unequivocally reaffirmed the applicability of international law in cyberspace. The current discussion focuses primarily on *how* international law applies.

State behaviour based on compliance with international law fosters stability in international relations. A better understanding of how international law applies in cyberspace contributes to the strengthening of an open, secure, stable, accessible and peaceful cyber environment. In this respect, and based on its commitment to an international rules-based order, Sweden presents its general position on some of the areas of central importance to a safe and secure cyberspace. Sweden does not see a need for new rules regulating cyber activities. However, cyber technology may give rise to specific questions requiring further clarification.

---

[1] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/68/98 (2013), adopted by the UNGA Resolution A/RES/68/243; *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174 (2015), adopted by the UNGA Resolution A/RES/70/237; *Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security*, UN Doc. A/75/816 (2021); *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN Doc. A/76/135 (2021).

[2] Both Reports of 2021 were adopted by the UNGA Resolution A/RES/76/19.

Sovereignty

The principle of sovereign equality of States is also applicable to cyberspace. Within their territories, States have jurisdiction and the right to exercise authority within the framework of international law. At international level, States are independent and enjoy sovereign equality in relation to other States. State sovereignty provides a basic foundation for other principles and rules such as those governing the prohibition of intervention and the prohibition of the use of force. However, States also have an obligation to respect the sovereignty of other States, and a breach of this obligation would amount to a wrongful act and give rise to State responsibility.

A State's jurisdiction and authority apply to persons and objects within its territorial borders, including cyber-related activities. A State has a right to protect persons and objects within its territory, or otherwise under its jurisdiction, against interference by cyber means. A State's authority and jurisdiction include a responsibility not to allow knowingly its territory to be used for acts contrary to the rights of other States.

In general, Sweden is of the view that violations of sovereignty may arise from cyber operations that result in damage or loss of functionality. Altering and interfering with data without causing physical harm may also violate sovereignty.[3] Such acts include those directed against cyber infrastructure belonging to private individuals or entities. Interference with a State's inherently governmental functions may also constitute a violation of State sovereignty, including when undertaken with cyber means.

Whether an intrusion has in fact resulted in a violation of sovereignty needs to be assessed on a case-by-case basis taking into consideration the nature and character of the intrusion.

Non-intervention

The principle of non-intervention is a fundamental principle of international law also applicable in cyberspace. It is not expressly mentioned in the UN Charter but is a corollary of the sovereign equality of all States. In the Friendly Relations Declaration, the principle of non-intervention is explained as "No State or group of States has the right to intervene, directly or

[3] A view expressed in Rule 4 of the Tallinn Manual. Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., 2017.

indirectly, for any reason whatever, in the internal or external affairs of any other State."[4]

The prohibition of intervention is generally understood to include two elements: intervening in matters in which each State is permitted to decide freely, and the involvement of coercion. These elements were confirmed by the International Court of Justice (ICJ) in the *Nicaragua case*.[5] With regard to the latter, the Court held that the "element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State."[6] The prohibition of intervention is applicable between States and does not apply directly to non-state actors.

While coercion is not defined in international law, it must be distinguished from other acts that would not qualify as coercion, such as criticism or other ways of influencing through diplomatic means. What constitutes coercion in the cyber context may not be easy to determine, requiring a case-by-case assessment that takes the specific circumstances into account.

Use of force

The prohibition of the use of force is a cardinal rule of customary international law, also applicable in relation to cyber operations. In the UN Charter, Article 2(4) stipulates a prohibition of the threat or use of force. The only exceptions in the UN Charter are the inherent right of individual or collective self-defence if an armed attack occurs, or acts taken pursuant to a decision of the UN Security Council authorising the use of force.

Acts that constitute the use of force are not clearly defined in international law. The ICJ has declared that the provisions on the use of force are not dependent on the choice of means, but rather apply to any use of force

---

[4] *General Assembly Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, UNGA Resolution 2625 (XXV) 1970. The principle of non-intervention may also be derived from a reading of articles 2(4) and 2(7) of the UN Charter.

[5] ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),* Merits, Judgment, ICJ Reports 1986, p. 14, para. 205.

[6] *Ibid*.

regardless of the weapons employed.[7] The Court has furthermore distinguished the most grave forms of the use of force (those constituting an armed attack) from other less grave forms based on scale and effects.[8] A similar assessment of scale and effects may be made in relation to whether an act constitutes a breach of the prohibition of the use of force. While most cyber operations would not constitute use of force, such operations would be considered as such if comparable to the scale and effects of kinetic use of force. An assessment needs to be made on a case-by-case basis.

Under Article 51 of the UN Charter, States have a right of self-defence if an armed attack occurs. It is not a requirement under the right of self-defence that the armed attack use kinetic means, nor that the use of force in self-defence is limited to such means. An attack by cyber means may have the potential to constitute an armed attack if its scale and effects are comparable to an armed attack by kinetic means. The exercise of the right of self-defence needs to be reported to the Security Council. Any use of force in the exercise of self-defence, including through cyber means, needs to adhere to principles of necessity and proportionality.

Due diligence

As a corollary to their sovereignty, States have an obligation to not knowingly allow their territory to be used for acts contrary to the rights of other States. This well-established rule of international law, described by the ICJ in the *Corfu Channel case*, also applies to cyber operations.[9] A State's obligation to ensure that its territory is not used to harm other States has often been referred to as an obligation of due diligence.

Due diligence is a standard of conduct and not of result, requiring a State to act responsibly and to do anything feasible to fulfil this obligation. States must use all reasonable means to prevent its territory to be used for acts causing serious adverse consequences to other states.

---

[7] ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ Reports 1996, p. 226, para. 39.

[8] ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),* Merits, Judgment, ICJ Reports 1986, p, 14, para.195.

[9] ICJ, *Corfu Channel case* (United Kingdom of Great Britain and Northern Ireland v. Albania), Judgement of 9 April 1949, ICJ Reports 1949, p.4, p. 22.

The difficulties involved in discovering cyber activities by non-state actors may affect what a State knows or should have known about such activities. Taking these difficulties into account, Sweden believes that this obligation, in principle, includes situations in which a State should have known about harmful activities taking place from its territory.

State responsibility

An internationally wrongful act by a State entails the responsibility of that State under international law. The articles on State responsibility drafted by the International Law Commission constitute secondary norms of international law, identifying conditions when a State is internationally responsible for wrongful acts and the effects thereof.[10] The general norms on State responsibility apply also in relation to wrongful acts in the cyber context.

Technical difficulties pose new challenges in identifying those responsible for cyber operations, compared with kinetic operations, but the rules on attribution under the law of State responsibility also apply in a cyber context. Cyber operations conducted by State organs are attributed to the State, as are cyber operations conducted by persons empowered to exercise elements of governmental authority if acting in that particular capacity. A State is normally not responsible for the conduct of individuals not empowered to exercise governmental authority. However, in situations where non-state actors act on the instructions or under the direction or control of a State, that conduct is attributed to the State. Conduct not attributed to a State may nevertheless be considered an act of that State if that State acknowledges and adopts the conduct as its own.

Legal attribution must be distinguished from public attribution. Legal attribution is an integral part in the process to establish and characterise an act in legal terms, and there is no legal requirement to disclose any evidence in relation to the assessment of attribution of conduct. Publicizing a decision on attribution is the prerogative of sovereign States and is not a requirement under international law.

[10] International Law Commission, *Responsibility of States for Internationally Wrongful Acts* (2001).

A State responsible for a wrongful act is under an obligation to cease its behaviour and to make full reparation for the injury caused. When a State is injured by an internationally wrongful act it may respond by a variety of measures. Such measures include countermeasures against the responsible State to ensure compliance with its international obligations.

Recourse to countermeasures is subject to strict requirements under the law of State responsibility and includes measures otherwise prohibited by international law. Countermeasures must *inter alia* be proportionate in character and cannot include the use of force. There is no requirement for responsive measures to be similar in kind and they may include non-cyber means. Before resorting to countermeasures, the injured State must notify the responsible State. It should be noted that this rule also allows for countermeasures without prior notification when urgent measures are needed to preserve the rights of the injured State. This rule also applies to cyber operations.

Under certain strict conditions, a State is allowed to employ measures that would otherwise be in breach of an international obligation in order to safeguard an essential interest against a grave and imminent peril. This would also apply in a cyber context. Necessity will, however, only rarely be available to excuse non-performance of an obligation.

International humanitarian law[11]

Sweden is of the view that international humanitarian law (IHL) applies to cyber operations conducted in the context of armed conflict. An armed conflict may be of an international or non-international character, depending on the nature of the parties to the armed conflict. The application of the law of armed conflict is not limited to kinetic force. However, to fall within the scope of IHL, a cyber operation must show a sufficient nexus with the armed conflict.

IHL is not concerned with the legality of war and does not as such legitimise the use of force between States. IHL aims to regulate the conduct of hostilities and to protect those who are not, or no longer, participating in

[11] This section does not include the laws of Occupation and Neutrality.

hostilities, thereby reducing risks and potential harm to civilians and civilian objects as well as persons recognised to be *hors de combat*.

IHL requires parties to an armed conflict to distinguish between civilians and civilian objects on the one hand and military objectives on the other. The conduct of hostilities obligates parties to the armed conflict *inter alia* to comply with the principles of distinction, proportionality and precaution. 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.

In the framework of IHL, 'attack' is defined as an act of violence against the adversary whether in offence or in defence. The determination of an act of violence should be based on its effects rather than the means used. A cyberattack in the context of IHL would at least include cyber operations that are reasonably expected to cause injury or death to persons or damage or destruction to objects.[12] Civilians are protected against attacks but only as long as they do not take a direct part in hostilities. A civilian may thus become a military target if taking a direct part in hostilities by the use of cyber means. In case of doubt whether a person is a civilian, that person shall be considered to be a civilian.

Cyber operations in the context of an armed conflict need to comply not only with rules governing the conduct of hostilities; certain persons, objects and activities are subject to special protection, such as medical personnel and units, including their cyber infrastructure, and religious or humanitarian personnel and objects.

International human rights law

Human rights apply online as they do offline. It is a well-established principle, first expressed in the 2012 Human Rights Council resolution on *The promotion, protection and enjoyment of human rights on the Internet*.[13]

---

[12] *Tallinn Manual 2.0*, Rule 92. Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., 2017.

[13] HRC Resolution, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/20/8 (2012), and subsequent resolutions, adopted by consensus.

The same human rights responsibilities and obligations that States have in the physical world also apply in the digital world. Although human rights are universal and indivisible, some are particularly relevant to the use of the internet, including (but not limited to) freedom of opinion, expression and information, freedom of association and assembly, and privacy. To enable the full enjoyment of human rights online, it is crucial that the internet remains open, free and secure with equal access and inclusiveness for all. The digital divides, including the gender digital divide, need to be closed. The internet should be governed through a multi-stakeholder approach.