May 28, 2021

Ministry of Foreign Affairs of Japan

Basic Position of the Government of Japan on International Law Applicable to Cyber Operations

1. Status and Purpose

Between 2004 and 2017, five Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), composed of experts appointed by the Secretary-General of the United Nations (UN), were established based on UN General Assembly resolutions. The GGE reports of 2013 and 2015 agreed by consensus by the governmental experts affirm that existing international law, in particular the UN Charter in its entirety, is applicable to cyber operations[1]. By the endorsement of the reports by consensus at the UN General Assembly, this affirmation has become the consensus view of all UN Member States. In the 2015 report, the group offered various important views on how international law applies to cyber operations. The group also recommended continued study on how international law applies. The fifth GGE failed to adopt a report in 2017, one of the reasons for which was that discussions on the application of international law did not achieve a sufficient convergence of opinions. From 2019, the sixth GGE[2] had intensive discussions on how international law applies. Its report was adopted by consensus on May 28, 2021.

This document summarizes the basic position at the moment of the Government of Japan on international law applicable to cyber operations. It was prepared as a national contribution at the request of the Chair of the GGE on the assumption that it will be included in the annex to the group's report to be submitted by the Secretary-General to the General Assembly pursuant to the mandate specified in Resolution 73/266, which requested the Secretary-General to establish the GGE. In this document, the Government of Japan reaffirms that existing international law, including the UN Charter in its entirety, is applicable to cyber operations, and states its present position on how existing international law applies to cyber operations focusing its views on the most important and most basic matters. The contents of this document take into consideration the discussions held by the six GGEs including the current one (governmental experts were appointed from among officials of the Government of Japan to serve on four GGEs, including the current one) and by the Open-ended Working Group (OEWG), which was established in 2019; the discussions held in bilateral and multilateral consultations between the governments of Japan and other States; the results of non-governmental research activities, including Tallinn Manuals 1.0 and 2.0, which were prepared by experts, including those from non-NATO States such as Japan, in their personal capacity with the support of the NATO Cooperative Cyber Defence Centre of Excellence; and the discussions held in multi-stakeholder fora, including ones led by Japan.

The Government of Japan hopes that the announcement of a basic position on international law applicable to cyber operations by the governments of many States and the application of international law in international and domestic courts and tribunals will deepen the shared international understanding on how international law applies to cyber

[1] In this document, the term "cyber operations" refers to operations using information and communication equipment and technology.
[2] The official name for the sixth GGE is GGE on Advancing responsible State behavior in cyberspace in the context of International Security.

operations. The Government of Japan also hopes that the deepening of a shared understanding — particularly regarding which activities in cyberspace constitute a violation of international law and which tools are available under international law for States whose legal interests have been infringed by cyber operations — will deter malicious activities in cyberspace.[3] The Government of Japan's policy is to continue actively participating in relevant discussions, including ones held under the auspices of the UN.

It should be noted that international law applicable to cyber operations is not limited to those mentioned in this document. The Convention on Cybercrime, to which Japan is a party, is an important element of international law applicable to cyber operations. Treaty provisions related to the Data Free Flow with Trust principle, for which Japan is promoting rule-making under the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the Japan-U.S. Digital Trade Agreement, and the Japan-UK Economic Partnership Agreement, also constitute international law applicable to some aspects of cyber operations.

2. International Law Applicable to Cyber Operations

(1) Existing international law and the UN Charter

Existing international law, including the UN Charter in its entirety, is applicable to cyber operations.

The 2015 GGE report mentions 11 voluntary, non-binding norms of responsible State behaviour. These items were agreed by Governmental experts as requiring implementation at least as norms, but they include items which affirm or relate to rights and obligations under international law. The inclusion of such norms among the 11 items does not mean that the rights and obligations under existing international law are extinguished or altered.

(2) Violation of sovereignty and the principle of non-intervention

A State must not violate the sovereignty of another State by cyber operations. Moreover, a State must not intervene in matters within domestic jurisdiction of another State by cyber operations.

With respect to the principle of non-intervention, cyber operations may constitute unlawful intervention when requirements including the element of coercion, which are clarified in the *Nicaragua* judgement *(1986),*[4] are met.

On the other hand, regarding a violation of sovereignty that does not necessarily constitute an intervention, in the *Lotus* case, the Permanent Court of International Justice

[3] The term "cyberspace" does not imply the existence of a space which does not belong to real space.
[4] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p.97-98, paragraph 205.

held that a State may not exercise its power in the territory of another State,[5] while, in the *Island of Palmas* case, the Arbitral Tribunal stated as follows: "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."[6] Taking these and other judgments into account, the Government of Japan considers that there exist certain forms of violation of sovereignty which may not necessarily constitute unlawful intervention prohibited under the principle of non-intervention.

With respect to violation of sovereignty, the International Court of Justice (ICJ), in the *Nicaragua* case (1986), held that the United States had acted in breach of its obligation under customary international law not to intervene in the affairs of another State, and, in addition, that the United States, by directing or authorizing overflights of Nicaraguan territory, had acted in breach of its obligation under customary international law not to violate the sovereignty of another State.[7] In addition, in the *Costa Rica v. Nicaragua* case (2015), the ICJ cited the absence of evidence that Costa Rica exercised authority on Nicaragua ' s territory as the reason for dismissing Nicaragua's claim concerning the violation of its territorial integrity and sovereignty.[8] Considering these cases, it can be presumed that, in some cases, a violation of sovereignty constitutes a violation of international law even when it does not fall within the scope of unlawful intervention.

An act of causing physical damage or loss of functionality by means of cyber operations against critical infrastructure, including medical institutions, may constitute an unlawful intervention, depending on the circumstances, and at any rate, it may constitute a violation of sovereignty.[9] As various opinions were expressed on the relationship between violation of sovereignty and unlawful intervention at the sixth GGE and the OEWG, it is desirable that a common understanding be forged through State practices and future discussions.

(3) State responsibility

Internationally wrongful acts committed by a State in cyberspace entail State responsibility. An internationally wrongful act occurs when the conduct of a State consisting of an action or omission violates an obligation prescribed by primary rules of international law. In the case of cyber operations as well, there is an internationally wrongful act when a State violates primary rules, including the principles of sovereignty, non-intervention, prohibition of the use of force, as well as various principles of

[5] The Lotus case, PCIJ, Series A, No. 10, 1927, p. 18-19.
[6] Island of Palmas Case, Award, RIAA, Vol. II, p. 838.
[7] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p.136-139, paragraph 292.
[8] 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. 738, paragraph 223.
[9] Tallinn Manual 2.0 also mentions physical damage to or loss of functionality of cyber infrastructure as a case that may constitute violation of sovereignty.

international humanitarian law such as the principle of prohibition of attacks on civilian objects, and respect for basic human rights.

Below, some of the articles of the Articles on Responsibility of States for Internationally Wrongful Acts drafted by the International Law Commission (ILC) (hereinafter referred to as the "ILC's Articles on State Responsibility") are mentioned as a reference. However, it should be noted that the Articles have not been adopted as a treaty text and the question of whether or not each article reflects customary international law has to be closely examined.

(a) Attribution

There is an internationally wrongful act of a State when the act is attributable to the State under international law and when the act constitutes a breach of an obligation of the State under international law.

There are legal, political and technical aspects in discussing the attribution of conduct to a State with respect to cyber operations.

To invoke State responsibility under international law with respect to any act in cyberspace, it is necessary to consider whether the act is attributable to a specific State. On this topic, Articles 4 to 11 of the ILC's Articles on State Responsibility provide useful reference. As a general rule, in such cases as a cyber operation conducted by a State organ, the act is considered to be attributable to the State. A cyber operation conducted by a non-State actor is, in principle, not attributable to a State. However, according to Article 8 of the ILC's Articles on State Responsibility, the conduct of a person or group of persons shall be considered an act of a State if the person or group of persons is in fact acting on the instructions of, or under the direction or control of that State in carrying out the conduct.[10]

(b) Obligations of a State responsible for an internationally wrongful act

Regarding cyber operations as well, a State responsible for an internationally wrongful act is under the following obligations. First, the State shall cease the act if it is continuing. In addition, the State shall offer appropriate assurances and guarantees of non-repetition, if circumstances so require. Besides, the responsible State is under an obligation to make full reparation for the injury caused by the internationally wrongful act.

(c) Countermeasures and necessity

Under international law, it is permitted, under certain conditions, to take countermeasures against internationally wrongful acts.

In general terms, under international law, a State which has been injured by an internationally wrongful act of another State may take, under certain conditions, countermeasures in order to induce the responsible State to comply with (i) the obligation to cease the international wrongful act and (ii) the obligation to make reparation.

[10] Article 8 of the ILC's Articles on State Responsibility

General international law does not confine countermeasures to those with the same means as the preceding internationally wrongful act in response to which they are taken. Japan considers that this is the same for the countermeasures against internationally wrongful acts in cyberspace.

The Government of Japan is of the view that a State may invoke necessity under international law when the requirements shown in Article 25 of the ILC's Articles on State Responsibility are satisfied.

(4) Due diligence

States have a due diligence obligation regarding cyber operations under international law. Norm 13(c) and (f) and the second half of paragraph 28(e) of the 2015 GGE report are related to this obligation.

In the *Corfu Channel* case (1949), the ICJ referred to the existence of "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States".[11] In relation to cyber operations, the due diligence obligation in this sense has significance.

Furthermore, with regard to the concept of the due diligence obligation, the Alabama Arbitral Award (1872) held that "due diligence" ought to be exercised by neutral governments in exact proportion to the risks to which either of the belligerents may be exposed, from a failure to fulfil the obligations of neutrality on their part,[12] and, in the *Genocide Convention (Bosnia and Herzegovina v. Serbia and Montenegro)* case (2007), the ICJ seems to consider the nature of the obligation to prevent genocide under the Genocide Convention to be the due diligence obligation and referred to an obligation of the contracting States to exercise the capacity to influence the actions of persons likely to commit genocide to prevent genocide so far as possible.[13]

The outer limit of the due diligence obligation of territorial States with respect to cyber operations is not necessarily clear. By reference to these judgements related to the concept of the due diligence obligation, it seems necessary to consider on a case-by-case-basis the scope of the obligation taking into account such factors as the seriousness of the cyber operations in question and the capacity of the territorial States to influence a person or group of persons conducting the attacks.

In light of the above, at the least, for example, when a State has received a credible notification from another State of the possibility that a person or group of persons located in its territory and receiving from it financial and other forms of support may be involved in a cyber operation that may cause serious adverse consequences, such as damage to a target State's critical infrastructure, the due diligence obligation owed by the informed

[11] Corfu Channel case, Judgment of April 9th, 1949: I.C.J. Reports 1949, P.22.
[12] Alabama claims of the United States of America against Great Britain, RIAA, Vol XXIX, p.129
[13] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 221, paragraph 430.

State is presumed to include the obligation to exercise its capacity to influence the state-supported person or group of persons so as to prevent them from implementing such cyber operations.

One characteristic of cyber operations is the difficulty of making judgment as to attribution to a State. In this respect, the due diligence obligation may provide grounds for invoking the responsibility of the State from the territory of which a cyber operation not attributable to any State originated. It is possible at least to invoke the responsibility of such a State for a breach of its due diligence obligation, even if it is difficult to prove the attribution of a cyber operation to any State.

(5) Peaceful settlement of disputes, prohibition of the use of force, and the right to self-defense

(a) Peaceful settlement of disputes

Any international disputes involving cyber operations must be settled through peaceful means pursuant to Article 2(3) of the UN Charter. In addition, pursuant to Article 33 of the UN Charter, the parties to any dispute involving cyber operations, the continuance of which is likely to endanger the maintenance of international peace and security, must first of all seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice. In order to ensure the peaceful settlement of disputes, the powers of the Security Council based on Chapters VI and VII of the UN Charter and the functions of the other UN organs, including ICJ based on Chapter XIV of the UN Charter and the Statute of the International Court of Justice should be used in disputes stemming from cyber operations.

(b) Prohibition of the use of force

Under certain circumstances, a cyber operation may constitute the threat or use of force prohibited by Article 2(4) of the UN Charter. Pursuant to this article, all States shall refrain in their international relations from the threat or use of force. The Government of Japan presumes that as a general rule the threat of force refers to a State's act of threatening another State by indicating its intention or attitude of using force, without actually using force, unless its arguments or demands are accepted. The obligation to refrain from the threat or use of force in international relations is an important obligation relating to cyber operations.

(c) Right of self-defense

When a cyber operation constitutes an armed attack under Article 51 of the UN Charter, States may exercise the inherent right of individual or collective self-defense recognized under Article 51 of the UN Charter.

(6) International humanitarian law

International humanitarian law is also applicable to cyber operations.

In situations of armed conflict, the methods and means of warfare used by the parties to the conflict are subject to regulations under international humanitarian law. This extends to cyber operations implemented by the parties to the conflict. Several principles under international humanitarian law, including the principle of humanity, necessity, proportionality and distinction, are also applicable to acts in cyberspace. In paragraph 28(d) of the 2015 GGE report, those principles are referred to as "established international legal principles." This reference, considered together with the fact that this report affirms the applicability of existing international law, can be interpreted to affirm the applicability of those principles. Meanwhile, Article 49 of the Additional Protocol I to the Geneva Conventions stipulates: "'Attacks' means acts of violence against the adversary, whether in offence or in defence."[14][15] The Government of Japan understands that cyber operations that may cause the destruction or neutralization of military targets, for example, may also constitute "attacks" under international humanitarian law, depending on the circumstances.

In principle, the existence of an "armed conflict" is a prerequisite for the application of international humanitarian law. Under the Geneva Conventions, there is no particular definition of an "armed conflict," and therefore, whether or not a certain incident constitutes an "armed conflict" needs to be decided on a case-by-case basis, taking into account a number of elements, such as the manner of the actual attack and the intent of each party to the incident, in a comprehensive manner. If the effects of cyber operations are taken into consideration, the conduct of cyber operations alone may reach the threshold of an "armed conflict."

As affirming the applicability of international humanitarian law to cyber operations contributes to the regulation of methods and means of warfare, the argument that doing so will lead to the militarization of cyberspace is groundless. For example, cyber operations during armed conflict that cause physical damage or loss of functionality to medical institutions may constitute a violation of international humanitarian law[16] and therefore should be appropriately regulated. On the other hand, modes of combat in cyberspace are different from those in traditional domains. Therefore, how international humanitarian law regarding, for example, the scope of combatants applies to cyberspace should be further discussed.

(7) International human rights law

International human rights law is also applicable to cyber operations. Individuals enjoy the same human rights with respect to cyber operations that they otherwise enjoy. Pursuant to international human rights law, States are under the obligation to respect human rights. The human rights that must be respected in cyberspace include all human rights that are recognized under international human rights law, such as civil, political,

[14] "Attacks" means acts of violence against the adversary, whether in offence or in defense (Article 49 of the Additional Protocol I to the Geneva Conventions).

[15] Tallinn Manual 2.0 stipulates that "a cyberattack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." (Tallinn Manual 2.0., Rule 92)

[16] For example, Article 12 of the Additional Protocol I to the Geneva Conventions

economic, social and cultural rights. The human rights that are particularly relevant in the context of cyberspace include the right to privacy, freedom of thought and conscience, freedom of expression, and guarantee of due process. The final sentence of paragraph 28(b) of the 2015 GGE report affirms the above. While Norm 13(e) of the report affirms some of the obligations under international human rights law, it does not change the obligations that are not mentioned therein.