Statement by Mr. AKAHORI Takeshi, Ambassador for Cyber Policy of the Ministry of Foreign Affairs of Japan, on the occasion of the virtual informal meeting of the OEWG on ICTs (September 30, 2020)

(Second intervention during the session on International Law)

I would like to take the floor for the second time to react to statements by other delegations.

First, I thank the French delegation for announcing the proposal for the creation of a Programme of Action (PoA). Japan is pleased to co-sponsor, sharing the belief that implementation of the 2013 and 2015 GGE reports is important. As Ambassador Verdier clearly stated, the proposal is to have the creation of a PoA included in the final report of this OEWG. It is not intended to put an end to the ongoing discussions in the OEWG. Quite on the contrary, we should continue to discuss the draft report in front of us and complete the work of this present OEWG.

Second, I sensed that many delegations feel the lack of sufficient discussions on "how" or even "how exactly" international law applies in cyberspace. Japan is now working on a national position paper on this question. I agree that national position papers will contribute to deepening understanding on how international law applies. However, we do not need to wait for our documents. Lack of a long description on how international law applies in the 2015 GGE report or in the text before us does not mean that delegations are not discussing how international law applies. It is in the spirit of contributing to a consensus report that many delegations are making limited comments to the text.

"The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" provides an excellent basis for Member States to clarify their positions on how international law applies in cyberspace. It is indeed the work of an international group of experts, mainly from NATO countries, but Japanese, Chinese and ROK scholars were involved. Governments need not agree to all the rules proposed by academics. Governments might consider different formulations for the rules they accept in principle. Discussing whether delegations agree on each proposed rule might allow us to have in depth discussions on how exactly international law applies. Today, I would like to read out 10 of the proposed 154 rules which seem most relevant to the discussions that we are having during this session.

・rule 14 - Internationally wrongful cyber acts

A state bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation.

・rule 15 - Attribution of cyber operations by State organs
Cyber operations conducted by organs of a State, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State.

・rule 28 - Reparation (general principle)
A responsible State must make full reparation for injury suffered by an injured State as the result of an internationally wrongful act committed by cyber means.

・rule 35 - Rights enjoyed by individuals
Individuals enjoy the same international human rights with respect to cyber-related activities that they otherwise enjoy.

・rule 65 - Peaceful settlement of disputes
(a) States must attempt to settle their international disputes involving cyber activities that endanger international peace and security by peaceful means.
(b) If States attempt to settle international disputes involving cyber activities that do not endanger international peace and security, they must do so by peaceful means.

・rule 68 - Prohibition of threat or use of force
A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful.

・rule 71 - Self-defence against armed attack
A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects.

・rule 76 - United Nations Security Council
Should the United Nations Security Council determine that a cyber operation constitutes a threat to the peace, breach of the peace, or act of aggression, it may authorise non-forceful measures, including cyber operations, in response. If the Security Council considers such measures to be inadequate, it may decide upon forceful measures, including cyber measures.

・rule 92 - Definition of cyber attack
A cyber attack 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.

・rule 94 - Prohibition of attacking civilians
The civilian population as such, as well as individual civilians, shall not be the object of cyber attack.

When delegations state that a certain principle or area of international law (State responsibility, prohibition of the use of force, self-defense, human rights, international humanitarian law, etc.) applies in cyberspace, they know that they are affirming the sense of certain proposed rules which I read out.

I am not asking to add the above ten rules to the text under negotiation, but I hope that my remarks here support some of the substantial proposals made by colleagues on the applicability of certain principles or areas of international law. We are indeed discussing how international law applies, and we should continue these discussions among us in this OEWG.