Statement by Mr. AKAHORI Takeshi, Ambassador for United Nations Affairs and Cyber Policy of the Ministry of Foreign Affairs of Japan, at the United Nations Security Council Open Debate on Cyber Security

June 29, 2021

Japan would like to express its sincere appreciation to H.E. Ms. Kaja Kallas, Prime Minister of the Republic of Estonia, for organizing this Open Debate on Cyber Security. Japan thanks Estonia for recognizing in its concept note the Open Debate on Complex Contemporary Challenges to International Peace and Security organized in 2017 under Japan's Presidency.

Japan welcomes the adoption of the OEWG report in March and the adoption of the report of the sixth GGE in May, both by consensus.

The greatest value of the OEWG report was that it was adopted by consensus in a process where all UN Members could participate fully. The UN Members affirmed the acquis directly, including that international law, particularly the UN Charter in its entirety, is applicable in cyberspace.

The GGE report has additional value. For each of the 11 norms included in the 2015 GGE report, the new report provides guidance and examples of implementation. Japan hopes that this content will further promote cooperation between States in advancing responsible State behaviour. In addition, it is clearer now that internationally wrongful acts attributable to a State entail State responsibility. The applicability of international humanitarian law is expressed in a clear manner. The Group noted again the inherent right of States to take measures recognized in the Charter.

We look forward to deepening concrete discussions on the application of international law in cyberspace in various fora in the future. Japan hopes that the position paper which it provided to the GGE compendium of national positions will contribute to such discussions. Here, I would like to share the most essential points in Japan's position.

Japan takes the view that a State must not violate the sovereignty of another by cyber operations. Moreover, a State must not intervene in matters within domestic jurisdiction of another State by cyber operations. Internationally wrongful acts committed by a State in cyberspace entail State responsibility.

States have a due diligence obligation regarding cyber operations under international law. Norms 13(c) and (f) and the second sentence of paragraph 71(g) of the 2021 GGE report are related to this obligation. Regarding the recent Colonial Pipeline incident, the U.S. President mentioned efforts toward "sort of an international standard that governments knowing that criminal activities are happening from their territory move on those criminal enterprises." We recognize the difficulty of attributing cyber operations to a State. 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.

Any international dispute involving cyber operations must be settled through peaceful means pursuant to Article 2(3) of the UN Charter. 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 should be used in disputes stemming from cyber operations. Japan has reservations to the idea of establishing a new international mechanism for attribution.

Japan's view is that 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 the same Article. International humanitarian law is applicable to cyber operations. This affirmation contributes to the regulation of methods and means of warfare. The argument that the affirmation will lead to the militarization of cyberspace is groundless.

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.

On the relationship between international law and voluntary norms, for the stabilization of cyberspace, it is essential that international law and norms work together to prevent internationally wrongful acts using ICTs and to promote responsible State behavior in cyberspace. As clearly expressed in the OEWG report, norms do not replace or alter States' obligations under international law.

Japan hopes that a large number of UN Members will voluntarily publish their national positions on how international law applies.

Japan believes that it is time to prioritize implementation of the agreed voluntary norms and obligations under international law, together with confidence building measures and capacity building measures.

In the context of implementation, Japan would like to invite Governments to proactively announce their legal assessment when a malicious cyber operation occurs, including, inter alia, on whether it constitutes a violation of international law. Such practice will promote shared understanding on how international law applies to cyber operations. Application of international law by international and domestic courts and tribunals to cyber incidents would have similar effect. It is Japan's hope that malicious activities in cyberspace will be deterred by accumulating such practice.

Japan strongly supports the Program of Action. We believe that the PoA will be an effective mechanism to secure and monitor implementation of agreed norms, obligations under international law, CBMs and capacity building. We look forward to deepening discussions on the PoA. We will also continue to participate proactively in the new OEWG.

Japan is committed to safeguarding a free, fair and secure cyberspace and will continue to actively contribute to discussions and efforts to promote rule of law in cyberspace, including at the United Nations.