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(June 2020) (including new proposal at the end)

【Threats】

Japan wishes to extend its gratitude to the Chair, Ambassador Lauber, and the UN Office for Disarmament Affairs for convening this important meeting of the OEWG despite the COVID-19 pandemic. Japan supports the Chair's efforts to continue our dialogue and identify further areas of convergence. We appreciate the hard work put in the preparation of the second pre-draft by the chair and by the support team.

Japan thanks the Chair for proposing a new roadmap for the OEWG. Japan is ready to accept a realistic revision of the roadmap, in a way that does not affect the complementarity between the OEWG and the GGE. And I heard today the thinking of the Russian Federation carefully. I look forward to further communication from the chair which was promised at the opening remarks. In the meantime, let's discuss substance following the chair's agenda and not spending too much time creating new mechanisms or processes.

I would like to start by referring to the "Introduction" part. Cyberspace is a place where we can freely create and share a wide variety of information and data across borders, regardless of location and time constraints. Anyone who is active in this space is able to create new value and freely interact with other entities. Emerging technologies, such as Artificial Intelligence, 5G wireless technology, quantum and cloud computing, which rely on cyberspace as a common good, provide innovative solutions for social and economic development and ample opportunities for human progress and transformation of societies and economies. Meanwhile, the development in ICTs is coupled with the increasing impact by and amplified vulnerability to misuses of such technology for purposes that are inconsistent with the objectives of maintaining international stability and security.

Mr. Chair, you asked us in your letter whether the current global situation revealed additional or amplified existing threats. I would say that the current health crisis is accelerating the societal trend towards digitalization while accentuating its risks and pertinent issues. I believe that paragraph 4 of the pre-draft could use words like accentuation or amplification of these issues or problems. We hope in any case that report will reflect a common understanding of the threat posed by malicious cyber activities in light of the aforementioned dynamics.

In order to reap benefits of ICTs for humanity while correctly and effectively addressing the existing and potential threats pertaining to the malicious use of ICTs, Cooperation with the private sector, academia, NGOs and other diverse stakeholders remains to be crucial, as is elaborated correctly in paragraph 11 of the pre-draft. Based on such recognition, during the intersessional consultative meeting last December, Japan was happy to invite several Japanese companies has brought in Japanese firms such as Hitachi, Fujitsu and NEC who made valuable contributions to the discussions.

Japan welcomes that in many paragraphs of the "Introduction" part, sentences start with the subject "The OEWG." This seems to be the ideal word when there is consensus on the content of a sentence. However, in many paragraphs in the rest of the pre-draft, the word "States" is used as a subject, without distinguishing the extent of support to a particular position. We should distinguish between an affirmation with a vast majority of support or a description of different positions in the Group. When there is an agreement, we should use "The OEWG", we could use "The OEWG" as a subject. When there is wide support, we might choose "many Members". When a limited number of Members support, we might choose "some Members". But I intend to agree with US delegates that we are not trying to create a verbatim record but a consensus report.

I would now like to address issues pertaining to existing and potential on threats. Japan cannot condone cyberattacks and malicious cyber activities which take advantage of the present crisis, including, as reported, ransomware striking medical institutions and authorities, as well as distributed denial of service attacks against medical re-search facilities. Such concerns were raised across the board at the UNSC Arria-formula meeting last month hosted by Estonia. It is such strong conviction that has prompted Japan to cosponsor a joint proposal together with the Czech Republic, Australia, Estonia, Kazakhstan and the United States on affirming a collective understanding that medical services and medical facilities are regarded as critical infrastructure for the purposes of norms (f) and (g), as we would like to further highlight in the upcoming sessions on the norms discussions. In addition, Japan supports paragraph 22 of the pre-draft which deliberates on the potentially devastating human cost of attacks on critical infrastructure and critical information infrastructure including medical facilities.

It is important to note that our concern lies not with the technologies themselves but with the misuse of such technologies by malicious cyber actors, that is why we support the pre-draft under paragraph 21. In the same vein, we strongly support the fact that the phrase “militarization of the digital space” has been removed from paragraph 18 of the pre-draft.

【Norms】

Japan supports the statement in the pre-draft that voluntary, non-binding norms set standards regarding the acceptable and unacceptable behavior of States in their use of ICTs, thereby increasing predictability and reducing risks of misperceptions.

All UN Members have agreed to a set of norms regarding responsible State behavior proposed by the Governmental Group of Experts in 2015, by the adoption of the relevant GA resolution “by consensus”. Upholding these 11 norms is the foundation for our

discussions.

We must work to elaborate on how to steadily put these norms into practice. It is important to build additional common understanding on the agreed content in previous GGE reports. Implementation of the existing norms enhances stability in cyberspace. The OEWG should not include language in the report which would undermine the existing consensus 11 norms.

Japan does not entirely exclude the possibility of creating new norms in the future. However, Japan expresses reservation about some parts of paragraph 38. Japan believes that norms established in the GGE report are not linked to specific technology or technical standards and do not risk becoming obsolete.

We would also like to point out that language in paragraph 39, which mentions that "States welcomed a set of 13 rules, norms and principles of responsible behavior of States" "in General Assembly resolution 73/27" is divisive and misleading. This OEWG should be a place to seek common understanding regardless of the different votes on resolution 73/27. That resolution was not by consensus. Let us continue supporting the very important 11 agreed norms endorsed by consensus by the General Assembly.

Paragraph 40 and its reference to the international code of conduct for information security tabled in 2015 also seems to undermine the existing 11 agreed norms. We wish to also point out that there is no consensus in the OEWG to recall General Assembly resolution 2131 of 1965.

The OEWG should pay careful attention to paragraph 42. The proposals listed in this paragraph are at this stage a mixture of (a) those intended to provide guidance on how to operationalize the 11 existing norms and (b) those intended to create new additional norms.

The proposals for new norms especially require careful consideration by each Member of the Group. To clarify, Japan would like to emphasize that its joint proposal on medical facilities and critical infrastructure, as is referred in the non-paper, is intended to offer guidance on how to operationalize the existing norms (f) and (g).

Japan supports the proposal by Canada to provide guidance to the 11 norms in the OEWG report. The guidance should be concise but operationally useful. I would like to make a new proposal here, which I will submit by writing later[1]. With regard to norm (i) on ensuring the integrity of the supply chain, Japan proposes the following language to be added as guidance, not as a new norm: "States have the right and responsibility to ensure the use of trusted suppliers and vendors for ICT equipment and systems, particularly to address national security concerns and protection of privacy. Reasonable steps may include legislation or administrative measures to secure supply chain security, to support development of reliable and trustworthy technology and industry, to diversify suppliers."

I thank you, chair.

---

[1] Japan's new proposal to the OEWG is to add the following language as guidance to norm (i) on ensuring the integrity of supply chain: "States have the right and responsibility to ensure the use of trusted suppliers and vendors for ICT equipment and systems, particularly to address national security concerns and protection of privacy. Reasonable steps may include legislation or administrative measures to secure supply chain security, to support development of reliable and trustworthy technology and industry, to diversify suppliers."