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

November 17, 2020

【Confidence Building Measures】

Thank you Chair.

I will not comment on the votes in the First Committee. Let us continue to discuss content, and successfully conclude this OEWG. I am happy that the majority of speakers are discussing substance of the draft report.

Japan unconditionally supports the Chair’s efforts to continue our important work.

Japan fully supports the content of the section on confidence building measures in the draft report in front of us.

Japan welcomes the reference to the 1988 Guidelines for Confidence-building Measures developed by the UN Disarmament Commission and endorsed by the General Assembly in consensus resolution 43/78(H).

Japan recognizes the significance of such measures as regular dialogue and voluntary information exchanges on existing and emerging threats, national policy or doctrine, national views on how international law applies to State use of ICTs, and national approaches defining critical infrastructure or categorizing ICT-related incidents. Such confidence building measures contribute to avoiding confrontation and to enhancing the free, fair and secure nature of cyberspace.

Regarding the question from the Chair on how to best facilitate cooperation on CBMs, I would like to reiterate the importance of cooperation through regional organizations or forums.

Japan, as one of the co-chairs of the ARF ISM on ICT security, has initiated several CBM activities within the ARF. These include, (a) the establishment of a directory of points of contact, (b) sharing of information on national laws, policies, best practices and strategies as well as rules and regulations, (c) awareness-raising and information sharing on emergency response to security incidents, and (d) organizing workshops on principles of building security in the use of ICTs in the national context.

Regarding the other question from the Chair on the most effective operational modalities of a directory of points of contact including security provisions, I would propose that we do not spend too much time and effort to creating a perfect directory. In the cyber era, we as individuals have virtually no place to hide. And I stress the word “virtually”. My official e-mail address is so easy to guess both to my friends from the past and to cybercriminals. Coming back to the global directory of POCs, regularly updating names of individuals, phone numbers and e-mail addresses is key to effective operationality. Governments might consider creating e-mail addresses linked to the office serving as the point of contact which will not change each time the individual in charge changes. Japan will certainly do so.

Let us remind ourselves that the global nature of the directory is essential and will be the novelty of this OEWG report. Cyber incidents do not always happen between States in the same region. Not
all States belong to a regional organization. For example, Japan participates in the ASEAN Regional Forum, but is not a member of ASEAN. Let us build upon the good experience of regional organizations but create the global directory.

I must point out, though, that success of cooperation through national points of contact depends largely on trust. Cooperation through points of contact would be inefficient if there is a continued pattern of malicious activity from one side. Chair, you correctly mentioned the need to look at the agenda of the OEWG comprehensively. I must stress that willingness by all States to adhere to norms of responsible State behavior and obligations under international law is a prerequisite of successful confidence building.

I thank you, Chair.