Joint proposal to amend Rev.1 text on CBMs

Submitted to the Chair on 27 July 2022 by the open, informal and cross-regional group of states to advance CBMs within the OEWG (Australia, Brazil, Canada, Germany, Israel, Mexico, the Netherlands, the Republic of Korea and Singapore)

10 a) Recalling the recommendation of the previous OEWG report (A/75/816) and building upon existing PoC directories at the regional level, the OEWG could agree to establish a global, inter-governmental, points of contact directory on ICTs at the United Nations. States may, on a voluntary basis, provide points of contact (PoCs) at the diplomatic, policy and technical levels with due competence at the national level in ensuring security in the use of ICTs that could be reached in times of urgency, for example through hotlines. Such a directory would respect State sovereignty and be politically neutral. It would be updated regularly, and be secure, operational and complemented by enhanced interaction and cooperation between States as well as capacity-building such as table-top exercises where requested. The UN Secretariat could be requested to collect and disseminate to the OEWG best practices on operationalizing such a directory which would include experiences at the regional level.

b) Recalling the recommendation of the previous OEWG, States voluntarily engage in transparency measures by sharing relevant information and lessons in their chosen format and fora, as appropriate such as could continue to voluntarily share white papers, national strategies and policies including ICT capabilities as well as share information on national ICT institutions and structures, and national lists of critical infrastructure. The report of the Secretary-General on developments in the field of information and communication technologies in the context of international security as well as the UNIDIR Cyber Policy Portal could be avenues for the voluntary sharing of such information.

c) It was proposed that aspects of confidence-building could include stakeholder engagement such as cooperation with interested stakeholders, including businesses, non-governmental organizations and academia, ensuring the integrity of the supply chain, preventing malicious uses of ICTs tools and techniques, preventing the use of harmful hidden functions and the sharing of current threat information. Points of Contact in the private sector could be established as appropriate.

d) Cooperation between CERTs could continue to serve as a confidence building measure which may be strengthened and which includes the sharing and dissemination of good best practices on incident management. Cooperation to mitigate attacks on CI and other malicious ICT-related activity could also be enhanced.

e) States also made a variety of proposals for new CBMs on issues such as public-private collaboration; the coordinated disclosure of vulnerabilities, to facilitate discussions on the terminology related to security of and in the use of ICTs to promote understanding of different national practices and usage; the development of common understanding on a glossary of basic terms with the aim of reducing mistrust by building common understanding; and on the use of ICTs for the economic development of States in a fair and non-discriminatory environment. States continued to emphasize that the OEWG itself served as a CBM.
Recommended next steps

1. States continue exchanging views at the OEWG on the development and implementation of CBMs, including on the potential development of additional CBMs.

2 bis) States continue to put into practice the recommendations on CBMs made by previous OEWG and GGEs.

2. States agree to establish a global, inter-governmental, points of contact directory, building upon and complementary to existing regional efforts, and at the fourth and fifth sessions of the OEWG, to engage in further focused discussions on the operationalization of such a directory on a consensus basis, as well as engage in discussions on initiatives for related capacity building, taking into account available best practices such as regional and sub-regional experiences where appropriate.

3. The UN Secretariat is requested to collate best practices on the operationalization of a global points of contact directory, which could include experiences at the regional and sub-regional levels, and produce a report by the end of January 2023 with options for the development operationalization on the establishment of such a global directory by the end of January 2023 for consideration at the fourth session of the OEWG.

4. States are encouraged to submit, on a voluntary basis, information on their national POCs as part of their responses to either (a) the report of the Secretary-General on developments in the field of ICTs in the context of international security and/or (b) the National Survey of Implementation.

5. States are invited to submit to the UN Secretariat, on a voluntary basis, their views, suggestions and recommendations on the development of voluntary protocols, procedures, and standardised templates for exchange of information between points of contact at the technical and political levels. The UN Secretariat, is requested to collate and circulate all submitted information to delegations for discussion at the fourth session.

6. The OEWG Chair is requested to convene an inter-sessional meeting with States and interested stakeholders, including businesses, non-governmental organizations and academia, no later than the beginning of the fourth session, to discuss topics which could support and foster confidence-building, including, inter alia, ensuring the integrity of the supply chain, preventing malicious uses of ICTs tools and techniques, preventing the use of harmful hidden functions and the sharing of current threat information.

7. States are encouraged to continue, on a voluntary basis, to share white papers, national strategies and policies including ICT capabilities as well as information on ICT institutions and structures security agency mission and functions, and ICT strategies at the national or organizational level, and the legal oversight regimes under which they operate, including through the report of the Secretary-General on developments in the field of information and communication technologies in the context of international security as well as the UNIDIR Cyber Policy Portal as appropriate.