Joint Working Paper on the Establishment of a UN Cyber Points of Contact Network

Submitted on 05 July 2022 by Australia, Brazil, Canada, Germany, Israel, the Republic of Korea, Mexico, the Netherlands and Singapore to the United Nations Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025.

In order to provide an operational basis for the implementation of cyber confidence building measures (CBMs) at the UN level and reaffirming their importance to prevent conflicts and promote peaceful uses of cyberspace, this paper sets out recommendations on the establishment of a UN Cyber Points of Contact (PoC) Network. The recommendations are based on the OEWG-Report A/75/816 as well as the GGE-Reports A/68/98, A/70/174, and A/76/135; they are submitted in further elaboration of the recommendations made in the initial joint working paper of this group circulated in May 2022.

The establishment of a UN Cyber PoC Network would constitute a CBM in itself. Setting up this network would also be contributing to the implementation of further CBMs at the UN level as all CBMs rely on the availability of national PoC to handle information which is shared with the intention of increasing confidence, trust and security in cyberspace.

In approaching the establishment of a UN PoC network, the following elements should be considered by the OEWG:

1. **Institutional anchor**: In view of its institutional linkage with the Open Ended Working Group and its security policy expertise, the network should be run by the UN Office of Disarmament Affairs (UNODA). This would ensure that both the data required for initially setting up the network and the data to be communicated via the network once it has become operational is managed by a professional institution, which enjoys trust throughout the UN community of states.

2. **Launching process**: UNODA should call on all UN member states to nominate PoCs for inclusion in the global directory of the network. Every member state should be requested to communicate at least one, but ideally two or more, national PoCs including the PoCs email- and phone contacts. Participation in the network would be at UN member states discretion. Each Member state would also be free to decide on the number of national PoCs it wants to
nominate and to decide on the professional or institutional affiliation (these could be policy / technical / diplomatic level contacts) of its PoC or PoCs. States are encouraged to nominate PoCs that have already been assigned as PoCs in the context of existing regional or sub-regional frameworks where applicable. The network should be considered operational once at least 50 UN member states have communicated their PoCs to UNODA. Based on member states submissions, UNODA would compile the UN directory of Cyber PoCs. This directory would be available for use by UNODA and all UN member states participating in the network.

3. **Tasks to be performed by PoCs:** National PoCs should be available for receiving and sharing information via the UN PoC network.

4. **Initial use of the network:** UNODA should run a bi-annual communication check involving all national PoCs in order to ensure PoC-data is up to date and PoCs are available to receive information via this channel. Among the first uses of the network could also be the implementation of cyber exercises exposing national PoCs to various scenarios.

5. **Budgetary questions:** The establishment and administration of the network as well as the communication checks and exercises would require additional resources. Any associated budgetary implications would need to be considered by the UN Fifth Committee.

6. **Procedural steps:** The OEWG should include in its 2022 progress report a recommendation for the establishment of UN Cyber PoC network. Subsequently, the annual First Committee resolution on ICTs in the context of international security should reflect this recommendation and outline the practical steps to be taken as set out in this paper.