Canada's contribution on the capacities required to participate in the POC [Points of Contact] directory

Mr. Chair, Canada is grateful for the opportunity to share its views on the capacities required to participate in the POC [Points of Contact] directory. Canada share its views regarding the topics below:

(i) General views on the capacities needed

From Canada's experience, the main capacity that States need to participate in the POC directory is its ability to identify at the national level their diplomatic and technical POC. This ability comes with a clear internal structure where it should be feasible to identify the competent national agency that should be responsible for the nomination, either in the case of the diplomat POC or the technical POC.

This national authority should be well equipped to respond to the tasks that the POC directory might fulfill. As it was noted by UNIDIR's research "Operationalizing a Directory of Points of Contact for Cyber Confidence-Building Measures" there are 4 main tasks that a POC directory should aim at: (a) communication, (b) assistance in cooperation, (c) reporting, and (d) national coordination. Therefore, the capacities that any POC should develop must meet the tasks that the POC directory will identify to operationalize.

(ii) Capacities required for the effective participation of POCs in the POC directory

In terms of national capacities required for an effective participation, Canada considers that this should be tackled from the point of view of the country's national capacities to respond effectively once the POC is contacted. In this sense, it would be useful to tackle separately the capacities required for both diplomatic and technical purposes.

As for the diplomatic capacities, effective participation would consist in accessing the relevant networks at the national level in order to adequately transmit any message. For example, the diplomatic POC should be able to communicate effectively with high level officials at the MFA or other national entities such as the Presidency. For this, a clear and well established communication chain should be settled for when a diplomatic POC will be contacted. In addition, training on cyber diplomacy and cyber international policy should be provided to the POC and its team as a way to enhance its ability to channel any alert, inquiry or request for information.

Regarding the effective participation of the technical POC, it must entail having a clear picture of the cyber national structure in order to channel technical requests for information, investigate cyber incidents or solve cyber issues when is needed, among other related-tasks. Technical training is required to enhance the capacity of technical POC and its team to be able to timely and effectively share information within the relevant cyber national authorities.

Finally, capacities related to enhance knowledge on national policies, regulations, and procedures are key for both diplomatic and technical POCs. These skills are pivotal for when POCs would need to navigate domestic procedures in order to consult on, among others, incident response mechanisms.

(iii) Suitable actions for building such capacities, including, inter alia, tailored programs for identified POCs.

In Canada's view, capacity building for States that require additional guidance to nominate their POC will be vital to the living of the POC directory. This first step can be a challenge for several countries for which the nomination of a national POC requires to improve technical skills or political will.

Additionally, capacity building for the already nominated POCs is essential to the efficacy of the POC directory. To this end, Canada believes that following through with a dedicated program to the operationalization of the POC directory could be a necessary step that States should drive at the OEWG. Main characteristics of this program could be to provide:

1. Tailored training: This program should provide tailored training sessions for both diplomatic and technical POC that could enhance capabilities in both fields. The training should meet the tasks that the POC directory will fulfill. To this end, an open exchange with regional organisations is key to avoid duplication, seek complementarity and share lessons learned.
2. Annual-basis training: The program should consider providing annual training that targets recently nominated POCs. This practice would contribute to keeping the directory updated and fix the lack of handover that can happen in the cyber field. This practice could also contribute to keeping the directory updated since training could be provided on an annual basis to the POCs in charge in a specific year.
3. A continuous exercise mechanism: Ping' tests or other communication exchange exercises should be developed on a regular basis in order to measure the efficacy of the directory and improve coordination.