France’s views on the establishment of a global cyber points of contact (PoC) directory

Paper submitted by France to the 2021-2025 Open-ended working group on security of and in the use of information and communication technologies (2021-2025 OEWG).

In accordance with paragraphs 2 and 3 of “recommended next steps” under section E of the OEWG’s first annual progress report, the paper is to serve as a contribution to the Group’s continued discussions on the development of a global directory, and as a national submission for the elaboration of a background paper by the Secretariat.

France recalls its support for the implementation and development of confidence-building measures (CBMs), which are an integral part of the cumulative and evolving framework for responsible State behaviour in the use of information and communication technologies (ICTs)1.

As affirmed notably by the consensus final reports of the 2019-2021 Open-ended working group and the 2019-2021 Group of governmental experts (GGE), CBMs can foster trust, cooperation, transparency and predictability, avoid misunderstandings, reduce the risks of tensions, escalation and conflict, thereby promoting security and stability in the ICT environment2.

France welcomes the recommendation to develop a global, intergovernmental PoC directory as part of the 2021-2025 OEWG’s ongoing work on CBMs. The establishment of such a directory can be a key element to facilitate communication between States. It can thus advance the implementation of other CBMs, and of the norms of responsible State behaviour, notably those related to information sharing and cooperation to address ICT incidents.

As noted in the Chair’s summary of the discussions 2019-2021 OEWG3, the establishment of a global PoC directory should in particular take into account the need (i) to build on, and ensure complementarity with, existing networks at the regional level, (ii) to ensure the security of the directory, (iii) to avoid overly detailed arrangements and maintain a certain degree of flexibility, (iv) to conduct regular communication checks, and possibly scenario-based exercises, to ensure the PoCs remain updated and operational.

Work on the establishment of the global directory can indeed build on progress made to establish PoC networks at a regional level. For instance, in the context of the OSCE’s work on cyber-related CBMs, France takes part in the implementation of CBM 84, which foresees that participating States will “nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs”. France has provided national points of contacts, at the policy (Ministry of Foreign Affairs) and technical level (national cybersecurity agency, hosting the national CERT/CSIRT), to enable communications in this framework.

---

1 First annual progress report of the 2021-2025 OEWG, A/77/275, paragraph 2.
4 Decision no. 1106, PC.DEC/1106, and Decision no. 1202, PC.DEC/1202, of the Permanent Council of the OSCE, on OSCE confidence-building measures to reduce the risks of conflict stemming from the use of ICTs.
As indicated by paragraph 16(b) of the OEWG’s annual progress report, States that have nominated PoCs at the regional level could provide the same PoCs for the global directory. Meanwhile, the establishment of a directory at the global level also makes it possible to develop exchanges with States that are not members of regional organizations.

Taking into account the elements above, France would like to share the following views on the operationalization of the global points of contact directory:

- **While the nomination of PoCs should remain voluntary,** States should be encouraged to provide national PoCs to improve the global directory’s effectiveness. States could designate their national PoCs, for example, when submitting a national report to the Secretary General5, and/or when using tools such as the National Survey of Implementation.

- **Purposes of the global PoC directory:** the purposes of the directory could include, *inter alia*, (i) to reduce the risks of tensions by facilitating communication between States, (ii) to improve cooperation in response to harmful ICT activity, for example by facilitating the notification of incidents, (iii) to facilitate requests for assistance.

- **Type of contacts to be shared:** while States should remain free to determine which PoC to nominate, they could be encouraged to provide contacts at the diplomatic and policy level (MFA), and contact points in the technical agencies in charge of the management of ICT-related incidents (CERT/CSIRTs).

- **Contact data to be shared:** States should be invited to provide relevant data such as professional email addresses, phone numbers, etc. Forms could be prepared to guide States in providing the relevant data regarding their national PoCs (but these documents should remain voluntary and flexible).

- **Host of the PoC:** as suggested by a cross-regional group of States in a paper submitted in July 20226, France concurs that the directory could be hosted and managed by UNODA, as a trusted institution with expertise in cyber issues. UNODA would make the directory accessible to all States that have provided PoCs. To ensure the security of the contact data, the directory could be hosted on a dedicated portal, where delegates from participating States would be able to login.

- **Information sharing:** when the directory is operational, *templates* may be developed to facilitate communication on ICT incidents between PoCs, by indicating which type of information could be shared (nature of request, etc.). These templates should nonetheless remain voluntary and flexible to allow for exchanges and cooperation even if some information is unavailable7. The directory could also envisage sharing of best practices and explore possibility for joint action to avoid duplication with regional PoCs networks already existing in regional formats, such as the OSCE.

---

5 As Member States are invited to do, for example, by OP6 of A/RES/76/19.
6 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, Singapore to the 2021-2025 OEWG.
7 See Final report of the 2019-2021 GGE, A/76/135, paragraph 77(b).
• **Regular updates of the PoC:** States should be encouraged to notify changes in their national PoCs (for example no later than 30 days after the change has occurred), so that the directory stays up to date. Communication checks could be made, for example on a bi-annual or annual basis, to ensure the PoCs are functional.

• In addition, PoCs could be involved in occasional scenario-based exercises.

In addition to the establishment of such a directory, France also supports continued discussions on the development of CBMs, and on the ways and means to share information, where appropriate, with other stakeholders such as the private sector, to better address vulnerabilities and incidents.

France remains committed to the implementation and developments of CBMs and looks forward to further discussions on the matter in the upcoming sessions of the 2021-2025 OEWG.