View on the global Points of Contact network and directory on ICT security
- Italy -

With reference to the document "ODA/2022-00047/ICT-PoC report" on the submission of views from States on global Points of Contact (PoC) directory, ITALY wishes to highlight its experience in participating to networks of PoC at both regional and subregional level, notably:

- at EU level:
  - the network of Cyber Ambassadors and their link to both PSC and Coreper Ambassadors;
  - the CSIRT network (CNW) for technical information exchange on cyber incidents and threats (e.g. IoCs, TTPs, vulnerabilities, threat reports, etc.);
  - the Cyber Crisis Liaison Organisation Network (CyCLONe) for situational awareness and operational coordination in case of large-scale cyber incidents;
  - the NIS Cooperation Group (NISCG) for the exchange of best practices and policy follow-up analysis about large-scale incidents;
- within OSCE:
  - the Communication Network and related PoC to securely exchange information between the OSCE participating States, as well as to facilitate pertinent communications and dialogue on security of and in the use of ICTs.

Taking the above into consideration and recognising the transnational and transregional character of cyberspace, ITALY welcomes the Chair's initiative following the adoption by consensus of the 2022 OEWG Annual Report aimed at establishing a global PoC network and directory on security in the use of ICTs. In this regard, and taking into consideration past experience and best practices, ITALY wishes to underline that:

- States' participation to the network should be voluntary;
- two kinds of PoCs could be established, a diplomatic and a technical PoC, with different objectives, not interchangeable:
  (i) **Diplomatic PoCs** should hold cyber diplomacy positions in Ministries of Foreign Affairs, that is to say that their core activity is cyber diplomacy in all its relevant aspects (international negotiations, mediations, CBMs, representation of their country in relevant international processes etc..), with special focus on developing communication lines to take for the prevention or de-escalation of possible tensions resulting from cyber activities. They could also facilitate communications among technical PoCs whenever necessary. Depending on national legislation Diplomatic PoCs could also provide assistance on development of national cybersecurity policies and legislation and exchange on the international legislative framework. To increase coherence and promote convergence, Diplomatic PoCs should hold such position in all PoC directories to which the State participates to;
  (ii) **Technical PoCs** could be expression of National Cybersecurity Agencies/Authorities/Centers, which have the task to coordinate all national

stakeholders in case of national cyber incidents and crises. To this end, technical PoCs should operate 24/7. They should be able to provide, upon request, assistance at technical and operational level, depending on national legislation also at policy level. This assistance could range from the sharing of technical information, such as IoCs and TTPs, to the sharing of best practices in the development of national cybersecurity policies and legislation;

- both PoCs should be able to support info-sharing activities. As a first step, States could also opt for providing only one PoC, preferably the Diplomatic PoC;
- since international relations are based on trust, periodical meetings should be convened to facilitate capacity-building, information exchange, and sharing of best practices, as well as scenario-based discussions and table-top simulations;
- the directory of the Diplomatic and Technical PoCs should be available exclusively to other PoCs. Moreover, with regard to Technical PoCs, the designation of specific individuals should be avoided;
- specific templates and/or rules for information-sharing among PoCs should be developed to standardize and facilitate communications.

One of the challenges that a global PoC network and directory on ICT security faces could be the risk of duplication with other existing PoCs directories and related networks, for example within the EU, the OSCE, and the ASEAN Regional Forum. Maintenance of such directories is an additional challenge, hence avoiding duplication would help to diminish such risk. This goal can be achieved through appropriate coordination mechanisms among different initiatives, also facilitating cooperation among existing regional and subregional organizations and platforms. Initiatives such as the OSCE partners for co-operation, both from Asian and Mediterranean countries represent a best practice.

Italy would deem useful the establishment of a UN process aiming at:

- mapping all existing PoC networks and directories on cyber/ICT security at regional and subregional level, as well as to collect identified best practices and lessons learned;
- establishing, under the UN aegis, a mechanism to facilitate cooperation among the PoCs of respective member countries, also developing specific collaboration platforms by establishing synergies among National Cybersecurity Agencies / Authorities / Centers.