Establishing a Directory of Points of Contact (PoC)

SUBMISSION BY INDIA

Background
Focal Point or Point of Contact (PoC) is an individual/entity designated by a Member State for communication and liaison in a specific area. It has been a common practice for the Member States to nominate such PoCs in areas related to disarmament, arms control and non-proliferation. Prominent examples include PoCs for UNPoA and MilEx reporting and for resolution 1540 related matters.

2. The idea of establishing a PoC directory/network in the area of ICT security to prevent and address serious ICT incidents and de-escalate tensions in situation of crises has been discussed by the various Groups of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. They have stressed the importance of functioning National Points of Contact in their reports in 2013, 2015 and, most recently, in 2021. The 2021 Final Substantive Report of the Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security also examined the matter and made its recommendations.

3. Building on the work of the GGEs and the previous OEWG, OEWG on security of and in the use of information and communications technologies 2021–2025, agreed to consider the establishment of a global, intergovernmental PoC Cyber directory for enhancing interaction and cooperation between States.

Points of Contact (PoC) proposals
4. Various ideas related to the Global PoC Cyber directory were discussed and specific recommendations were proposed in the GGE Reports of 2013 (A/68/98), 2015 (A/70/174), and 2021 (A/76/135) and the 2021 Final Substantive Report of the OEWG (A/AC.290/2021/CRP.2). The salient points from the GGE & OEWG reports are as follows:
   - Identification and establishing dedicated National Points of Contact (PoC) as an important confidence building measure in the area of ICT security
   - Defining clear roles for these PoCs
• Creating inter- and intra-governmental procedures to ensure effective communication between PoCs during crises.
• Exchanging information on national PoCs to expand and improve existing channels of communication.
• Building regional and global network of Cyber PoCs

Utility
5. Establishing a global directory/ network of Cyber PoCs can contribute to developing practical measures to increase transparency and predictability in the area of ICT security, thereby promoting greater cooperation between member states and enhancing stability in the cyber domain.

6. The Cyber PoC global directory/ network will serve as a mechanism for enhanced sharing of information among States on ICT security incidents, incident response and mitigation, facilitated by secure and direct communications between States through the PoC network.

7. It will help reduce tensions, prevent misunderstandings and misconceptions that may stem from ICT security incidents, thereby preventing serious ICT incidents and de-escalating tensions in crisis situations.

8. The Cyber PoC directory/ network can also be a potential platform to support the development of early warning mechanisms related to ICT security, where States can receive, collect and analyse information on ICT security incidents for timely response, recovery and mitigation actions.

9. While the Cyber PoC directory/ network has traditionally been seen as an important Confidence-Building Measure (CBM), it can also contribute to provision of assistance and capacity-building in the area of ICT security. Capacity-building is essential for promotion of cyber resilience of member states and also confidence-building in the field of ICT security.

10. Having dedicated PoCs for assistance and capacity-building will enhance the prospects of direct communication between States on their needs and their ability to offer assistance or through the regional PoC networks. Such assistance can be extended in, but
not limited to, conducting cybersecurity risk assessment, preparation of incident response plans etc.

11. Cyber capacities can also be enhanced through regular sharing of experiences and best practices by PoCs in the area of ICT security, including on matters related to legal frameworks, enforcement etc.

Structure
12. In order to exploit the advantages of a Cyber PoC directory/ network, a multi-tier structure is recommended.

13. At the national level, Member States may find it useful to identify and nominate 3-categories of PoCs for the directory to ensure effective communication and collaboration:
   - **PoC (Operations):** They will serve as focal points on all issues related to ICT security incidents, response and mitigation. Typically, cyber agencies and institutions dealing with ICT related incidents can nominate such a focal point.
   - **PoC (Assistance):** They will serve as focal points for coordinating all assistance and capacity-building issues. Typically, the Foreign Ministries can nominate such a focal point.
   - **PoC (Policy/Legal):** They will serve as focal points for all policy and legislative matters related to ICT & ICT security. Typically, the Ministries in-charge of Cyber / Information Technology, who deal with national policies and legislations on ICT/Cyber, can nominate such a focal point.

14. The Cyber PoC directory should contain the name, designation, organisation, email and contact number (optional) of each category of PoC nominated by Member States. States can also consider nominating a back-up PoC for each category. Based on their national cyber structures and capacities, States can nominate common PoCs, who may perform all or multiple roles described above.

15. Recognising that the States in the region with the relevant expertise are usually the ‘first responders’ in crisis situations and also for capacity-building and assistance requests, Member States can consider inclusion of their PoCs in sub-regional/ regional Cyber PoC networks.
16. At a global level, the Cyber PoC directory should facilitate cross-regional communication and information sharing, particularly with the objective of real-time reporting of cyber incidents, development of early warnings related to cyber threats/ incidents and facilitation of assistance.

17. As part of the global directory, Member States may find it helpful to have PoCs from international organizations and other relevant stakeholders, who have expertise on ICT security, especially on policy and assistance matters.

**Operationalization**

18. In order to garner the support of all Member States and ensure the smooth operation of the Cyber PoC directory, it must be established and maintained under UN auspices. Due to its subject expertise and its continuing support to the inter-governmental cyber process, **UNODA is better placed to be the custodian of this directory.**

19. Ensuring that information on PoCs is up-to-date is critical to facilitate real-time exchange of relevant information and enable cooperation among Member States to build trust and confidence. Hence, **the PoC directory shall be mounted on an online portal, maintained by UNODA, dedicated to global cyber security cooperation.** This will facilitate ease of communication and ensure updated information of the Cyber PoC directory.

20. Once the portal is established, UNODA should invite all Member States to upload details of the 3-categories of PoCs, as part of the Global Cyber PoC directory. Member States can also choose to be part of a regional/ sub-regional PoC network, when uploading their PoC nominations to the portal. Participation in the global/ regional/ sub-regional PoC directory is voluntary and will be the discretion of Member States.

21. **Member States must have access to the portal through relevant user credentials, which would be shared by UNODA to Member States.** These credentials can be used by Member States to access the PoC directory, share/ exchange information and also update the PoC information on a regular basis. UNODA should send periodic reminders (every six months) to Member States to update their PoC information.

**Communication between PoCs**
22. Member States shall have the option of sharing or exchanging information directly through the portal or using the information available in the PoC directory on the portal to share or exchange information bilaterally through relevant channels.

23. When the information is shared through the portal, it would be essential to establish procedures for information sharing and response. For example, when a Member State PoC shares information related to policy and assistance matters, it should have the option of broadcasting it globally to all members of the PoC network, or transmit it only to a specific regional network, or share it bilaterally to specific country PoCs.

**Funding**

24. The establishment of the Cyber PoC directory, mounting it on a dedicated online portal and facilitating exchange of information/communication between PoCs through the portal would require additional resources – financial, technological and human. In order to ensure the sustainability and longevity of the PoC directory, this expenditure should be met from the UN regular budget. However, voluntary financial contributions can also be sought to enhance the effectiveness of the operations of the PoC directory and the online portal.

25. The OEWG should make suitable recommendations for the establishment of the Global PoC Cyber directory and the portal for its operationalisation to General Assembly, through the First Committee, to secure the required funding from assessed contributions to the UN budget.

**Follow-up**

26. Once the Cyber PoC directory is established, there must be periodic interactions between the PoCs to discuss the utility and modalities of sharing information using the PoC Cyber directory. Such interactions can happen on the sidelines of the OEWG 2021-2025 or future platforms for regular institutional dialogue between Member States on ICT security. Capacity-building of the PoCs must also be given due importance.

***