Submission of UK views on global points of contact directory pursuant to A/77/275
“Developments in the field of information and telecommunications in the context of international security” containing the progress report on the discussions of the open-ended working group on security of and in the use of information and communications technologies 2021-2025

In the first Annual Progress Report of the OEWG 2021-2025 (A/77/275), States agreed to:

- ‘establish, building on work already done at the regional level, a global, intergovernmental, points of contact directory; and
- engage in further focused discussions on the development of such a directory, on a consensus basis, as well as engage in discussions on initiatives for related capacity-building, taking into account available best practices such as regional and sub-regional experiences where appropriate’.

The UK supports the identification of concrete, action-oriented proposals to implement the UN framework for responsible State behaviour in Cyberspace, including the further elaboration of existing proposals regarding a global Points of Contact (PoC) Network and Directory at forthcoming OEWG sessions. We reiterate our belief that CBMs ‘can contribute to preventing conflicts, avoiding misperception and misunderstandings, and the reduction of tensions’. (A/75/816 para 41).

Our input is guided by the combined conclusions and recommendations of the consensus OEWG and GGE reports, alongside practical experience of the OSCE PoC network¹.

**Why have a global PoC network and directory?**

The UK recognises that ‘not all States are members of regional organizations or of regional organizations undertaking such work’ (A/77/275 para 16a) and that a global network and directory would ensure that all States can contribute to and benefit from enhanced international peace and security in cyberspace.

The primary function of such a network is to enable direct communications at times of crisis in order to protect international peace and security, as confirmed in previous OEWG and GGE consensus reports.

- ‘points of contact … that could be reached in times of urgency’. (A/77/275 para 16b)
- ‘facilitate secure and direct communications between States to help prevent and address serious ICT incidents and de-escalate tensions in situations of crisis’ (A/76/135 para 76)
- ‘help reduce tensions and prevent misunderstandings and misperceptions that may stem from ICT incidents, including those affecting critical infrastructure and that have national, regional or global impact’. (A/76/135 para 76)
- ‘address serious ICT incidents’; (A/70/174 para 16a)
- ‘… expand and improve existing channels of communication for crisis management…; (A/68/98 para 26c)

A secondary function of such a network is the resultant increase in ‘interaction and cooperation between States’ (A/77/275 para 16a).

**Who should participate in a global PoC network and directory?**

---

¹ A summary of OSCE’s work on implementation of CBMs, including through its PoC network was submitted to the 2019 OEWG. https://front.un-arm.org/wp-content/uploads/2020/04/1-osce-nonpaper-for-oewg-and-gge.pdf
Participation in such a network and directory must remain voluntary, but States should be encouraged to participate in one or more networks. Diplomatic PoCs are the key interlocutors for matters of international peace and security. PoCs must be suitably empowered to provide a coordinated, whole of government response.

We recognise existing regional initiatives to develop PoC directories, such as those of the OSCE, and consider that a global PoC network must remain complementary. Where individual Member State permission is given, it may be effective to allow regional organisations to share existing PoC information into the global network and directory.

Industry, non-governmental organizations and academia make significant contributions to confidence building and development of effective responses to crises. The technical community already provides many platforms for these contributions and as such, they do not need to be included in this specific network.

**What should a global POC network and directory do?**

A global PoC network/directory should support diplomatic PoCs to make direct contact with relevant international partners at times of crisis, in order to protect international peace and security. Whilst other networks have developed additional functions, this network should initially focus on its core function.

Whilst PoCs may voluntarily share national reports with counterparts, this network should not introduce requirements to provide reporting into the UN system or to other States. The Secretariat does not hold the appropriate expertise or mandate to provide a coordination or assistance function, which should remain with technical organisations and the relevant authorities. Direct contact will facilitate provision of assistance from member States, but such provision remains the prerogative of those States.

Extending communications to ‘business as usual’ support, communication and assistance will reduce the value placed on participation in the network. For this reason previous consensus reports have been careful to distinguish between PoC networks, CERT communities, law enforcement groupings, and mechanisms to share information etc. (e.g. A/68/98 para 26d, A/70/174 para 17a).

**How should the global POC network and directory operate?**

The Secretariat’s role should focus on the effective functioning of the network and directory, prioritising communications with Member States about the use of the network and maintenance of the effective functioning of the directory, including through reminders to keep it updated. Once the directory is created, such management tasks will be limited and primarily carried out by existing Secretariat staff within the course of their daily duties.

Additional cooperation between Member States and the Secretariat could support the effective operation of the network. This could include driving broad engagement through the sharing of best practice with regards to use of the network, facilitating face-to-face meetings between PoCs, or through conducting exercises. A/76/135 para 77 a-c and para 78 provide suggestions for such activities. This should be funded by voluntary contributions as required, rather than through a dedicated budget.

To effectively facilitate direct communication at times of urgency, the directory should be available on line. An access controlled, dedicated webpage of an existing UN site/platform, for instance the UNIDIR cyber policy portal, could facilitate direct updates. The directory would need to contain the following information about PoCs: Name of unit in charge of the PoC; General email of unit in charge; UN languages PoCs can receive messages in.