IMPLEMENTING CYBER CONFIDENCE MEASURES GLOBALLY
-TOWARDS THE UN POINT OF CONTACT DIRECTORY

Working Paper submitted on 25 November by
Australia, Brazil, Canada, Chile, Fiji, Germany, Israel, the Republic of Korea, Mexico, the
Netherlands, Singapore and Uruguay

In the 2022 Annual Progress Report (APR) of the Open-Ended Working Group 2021-2025, all UN Member States agreed to establish, building on work already done at the regional level, a global, intergovernmental, points of contact (PoC) directory. States further agreed on the next steps towards the establishment of such a PoC directory which include: focused discussions at the fourth and fifth sessions of the OEWG as well as discussions on initiatives for related capacity-building, a background paper prepared by the UN Secretariat about the views of States as well as the organization of an inter-sessional meeting dedicated to the topic.

Building on the input paper focusing on recommendations with regard to the establishment of a PoC directory submitted on 5 July 2022, this working paper of the open, informal and cross-regional group of states to advance confidence-building measures (CBMs) within the OEWG seeks to further contribute to in-depth discussions about a global PoC directory at the inter-sessional meeting of the OEWG to be held from 5 to 9 December 2022. In line with the 2021 OEWG report, which concluded that establishing national PoCs is a CBM in itself and useful for diplomatic, policy, legal and technical exchanges, as well as incident reporting and response, the paper proposes to address the following aspects at the meeting:

1) Interplay between regional PoC directories and a UN PoCs directory

As underlined in the 2022 APR, significant work on CBMs has been done at the regional level and a number of regional organizations have already developed PoC directories, providing points of contact at the diplomatic and/or technical level with due competence at the national level in ensuring security in the use of ICTs. The following three regional organizations provide examples of successfully established PoC directories within their frameworks:

OSCE: The Organization of Security and Cooperation in Europe (OSCE) established official PoCs in 2013 as part of the first set of CBMs, comprising national contact points at the technical and/or policy level. CBM 8 encourages all OSCE participating States to nominate PoCs to facilitate pertinent communications and dialogue on security of and in the
use of ICTs and as such provides the **basis for implementing the other 15 voluntary CBMs implemented within the OSCE context.**

**ASEAN Regional Forum (ARF):** The ASEAN Regional Forum (ARF) established the **Points of Contact Directory** on Security of and in the Use of Information and Communications Technologies in 2020 with Ministers’ approval. The directory comprises national contact points for both **senior level and working level** contacts. If an ARF Participant has a central agency or body nominated by their government to coordinate the nation’s conflict prevention, crisis management and response in relation to security of and in the use of ICTs, a point of contact should be established within this body to serve as single point of contact for all ICT security incidents of regional significance. For ARF Participants who do not have a single coordination PoC nominated by their government, the channels detailed below can be used. Given its purpose, covering both prevention and response, the Directory may hold entries for: diplomatic, national security and policy coordination, law enforcement and technical PoCs. Nomination of PoCs to the directory occurs on a **voluntary basis** and is **updated and ping-tested biannually.**

**OAS:** At the **Organization of American States (OAS),** one of the first measures adopted by the Working Group on Co-operation and Confidence Building measures in Cyberspace in 2018 was the **identification of national PoCs at the political level** to discuss the implications of hemispheric cyber threats. They should be distinct from and supplement the existing work of law enforcement and other technical experts. Information on PoCs shall be **updated annually,** or as frequently as needed. In 2019, the Working Group agreed further to designate **PoCs in Ministries of Foreign Affairs** to strengthen cooperation on cyber diplomacy and to facilitate international dialogue. At the OAS CBMS portal (https://oascybercbms.info/) members of the Working Group can access the list of PoCs and contact any registered PoC.

In order to **facilitate the establishment** of a global PoC directory, to **avoid duplication** of administrative efforts and to **ensure complementarity** with existing regional PoC directories, existing **national contact points at regional level should ideally be also nominated as contact points within the UN PoC directory.** Taking into account that **different categories of PoCs (technical, policy, diplomatic) may exist at regional level,** States could nominate the **existing PoC from the category it considers most suitable** for nomination at the global directory.

However, as recognized in the APR, **not all States are members of regional organizations** that have already **set up PoC directories,** which poses the challenge that **a number of states**
in Africa, Asia, Latin America, the Pacific and the Middle East are not part of such frameworks yet. Therefore, capacity-building could be envisaged, where necessary, for interested countries to nominate PoCs and in addition the OEWG could send a strong signal of encouragement to other regional organizations to develop PoC directories within their frameworks.

2) **Running communication checks**

To test functionality and to ensure that all data in the UN PoC directory is up to date, bi-annual communication checks should be held. These checks would not carry specific information, but simply make sure that all appointed PoCs at the national level are available under the indicated communication channels (email addresses and telephone numbers). States are requested to send updates about their PoCs to the administrative body. A respective reminder would be sent to all participating States on an annual basis.

So-called PING-tests (Packet Internet Groper) would measure the amount of time necessary for each PoC to respond to the communication check.

3) **Holding cyber exercises and trainings**

While the PoC directory would be a CBM in itself, it would also provide the ground for the implementation of other CBMs at the global level. As one example, cyber exercises and trainings relating to the implementation and operationalization of PoCs and this PoC directory could contribute to further building trust among states and at the same time produce valuable insights for strengthening national and regional cyber resilience through practical, cross-regional exchange.

Best practices and lessons learned at the regional level could serve as a starting point for designing the exercises and trainings.

4) **Communication, especially in times of crisis, and incident management**

Building on communication checks and cyber exercises, another core function of a future UN PoC directory could be the reporting of incidents and responses as well as communication in the event of crisis, which would complement and strengthen existing international and regional CERT-CERT PoC arrangements for the operational and technical exchange of cyber threat and cyber attack-related information. States would have the possibility to
share relevant information and lessons learned on a voluntary basis through trusted communication channels and thereby contribute to preventing cyber incidents in other countries or to managing a crisis effectively. Such additional CBMs would need to be subject to further focused discussions within the OEWG.

Also in non-crisis times, the PoC directory would enable communication among participating States, e.g. by serving as a resource for Member States to do outreach amongst each other, e.g. through virtual meetings for peer-to-peer exchange or by sharing information on events related to cybersecurity. Such interaction would equally increase trust and reduce the risk of misunderstanding.

5) Administrative issues to set up a UN PoC directory

Given its institutional linkage with the OEWG and its trusted role within the UN community, the UN Office of Disarmament Affairs (UNODA) would be most suited to set up and administer the UN PoC directory. Participation in the UN PoC directory would be at States’ discretion. All participating States would have full access to the data available in the PoC directory.

As a first step in the establishment of the PoC directory, States would be invited to nominate one or more diplomatic and/or technical PoCs and to communicate an email address and a phone contact of the designated expert or institution. As mentioned above, ideally States would nominate PoCs already assigned in existing regional or sub-regional frameworks where applicable. As both diplomatic and technical PoCs can be nominated, the OEWG membership should agree on their respective roles and functions.

Once a critical mass of at least 50 States has communicated information about their national PoCs to UNODA, the network would be considered operational and UNODA would compile the PoC directory. UNODA would then continue with communication checks to test its functionality.

For all functions to be performed to establish, administer and effectively use the PoC directory, UNODA would require additional financial resources. The relevant budgetary implications would need to be considered by the UN Fifth Committee.
6) **Way forward**

Building on the 2022 APR, which passed in consensus the decision about the future establishment of a UN PoC directory in principle, the open, informal and cross-regional group of states to advance CBMs within the OEWG proposes to agree on the detailed set-up and modalities of establishment of the PoC directory in the 2023 APR. The group advocates for taking UNODA’s background paper about States’ views as well as the results of UNIDIR’s Survey on PoC directories into account and expects to lay the ground for consensus language in the next APR through fruitful discussions at the inter-sessional meeting in December.