In response to the request of the UN Office for Disarmament Affairs for views on the global Points of Contact (PoC) Directory, Slovakia aligns itself with the statement delivered by the European Union. Nonetheless, Slovakia wishes to submit its contribution in the form of the following comments:

- As Slovakia has already indicated via the UNIDIR survey, Slovakia supports the establishment of the proposed global cyber PoC directory on security of and in the use of information and communication technologies (ICT) at the United Nations.

- Slovakia supports the identification of concrete, action-oriented proposals to implement the UN framework for responsible State behaviour in cyberspace. As such, the global PoC directory could play an important role in fostering capacity-building while, simultaneously, serve as a confidence-building tool. Slovakia believes that the PoC directory could aid with easing the palpably rising tensions and contribute to reducing the risks of use of ICTs.

- Slovakia underscores the importance of advancing confidence-building measures (CBMs) between countries that ‘can contribute to preventing conflicts, avoiding misperception and misunderstandings, and the reduction of tensions’ (A/75/816 paragraph 41). As stressed in the past GGE reports (2013, 2015, 2021), the recommendations of the 2021 OEWG report, and the Annual Progress Report of the OEWG 2021-2025 (A/77/275), the creation of a well-functioning PoC directory is a crucial part of operationalising CBMs at a global level.

- In order to expand and improve existing channels of communication for crisis management, the PoC directory should include two contacts for each State – political/diplomatic and technical. Each State could voluntarily assign a policy/political PoC (e.g. Ministries of Foreign Affairs) to follow up on matters related to political implications of ICT security and the implementation of the agreed normative framework within the United Nations. In parallel, States could also voluntarily assign a technical PoC from a relevant national agency/authority (e.g. national CERTs). Slovakia believes that appointing merely a technical PoC would not reflect the extent to which technical aspects of ICT security are nowadays intertwined with political considerations.

- Slovakia also encourages holding thematic workshops and tabletop exercises for the assigned PoCs before and after the establishment of the directory as some UN Member States willing to join the directory, could be first time adopters of PoCs.
• Importantly, the goals of the global PoC directory need to be clearly defined since Member States’ available resources and existing domestic structures vastly differ which might, in turn, influence the way in which States approach the directory, e.g., the number of PoCs nominated by each State.

• Slovakia does not view the global PoC directory as duplicating other dedicated networks for CSIRTs/CERTs. That said, it is crucial to draw on best practices and valuable experiences with regard to existing PoC networks from other regional organisations, such as the OSCE (CBM No. 8) and OAS. The complementarity and coordination with already existing efforts by regional organisations on CBMs and other initiatives to develop regional PoC directories on cyber and ICT security are of high importance. To avoid duplication of work and to capitalise on existing mechanisms, States could nominate existing, regional PoCs.

• As for the technical side of the portal, Slovakia would prefer a password-protected directory. The UN administration could be in charge of carrying out the technical tasks of updating relevant information on the platform. In this sense, a sufficient amount of resources should be allocated for the platform management. The information available could include: name, position/affiliation, email, phone, typology (i.e., diplomatic, operational and technical) and preferred UN language (noting that if States opt for a multilingual PoC directory, this would consequently need to be reflected in the financial and human resources dedicated to the platform management). The platform management also needs to be considered in a broader context with an aim to ensure continued operationalisation of the portal.

• Nominated PoCs could be approached on a bi-annual or annual basis in a form of, for instance, periodic “ping” exercises/tests or simple email to the contacts, requesting to confirm the receipt to check the PoC availability and to make sure the provided information is up to date. The Secretariat could then provide a brief report on the responsiveness of the existing PoCs so that also other States are aware of the level of engagement and participation. The network could then be evaluated in terms of its functionality and usefulness after one/two year(s) of its operation. Standard operating procedures could be developed in this regard.

• While Slovakia is fully aware that there are outstanding issues to be discussed, such as developing specific templates and rules for information sharing amongst the PoCs to standardise forms of communication, Slovakia is ready to provide our national contacts as soon as the PoC directory is finalised.