Thematic Session: POCs directory (Monday, 5 December)

Honorable Chair, Ambassador Gafoor

I have the honour to speak on behalf of the European Union and its Member States.

The Candidate Countries North Macedonia, Montenegro, Albania and the Republic of Moldova, the potential candidate countries Bosnia and Herzegovina and Georgia, and the EFTA country Iceland, member of the European Economic Area, align themselves with this statement.

Let me start by thanking you and your team for tremendous efforts during the past year in successfully leading this working group, and adopting, by consensus, the OEWG's Annual Progress Report.

Dear colleagues,

1. The EU and its Member States welcome the first Annual Progress Report of the second Open-Ended Working Group and express their support to the Chair to use this report to establish a concrete agenda and a clear roadmap for 2023, allowing the OEWG to make progress in its discussions.

2. We welcome the further discussion on how to develop and operationalize a global points of contact (PoCs) directory as agreed in the conclusions and recommendations of the 2021 OEWG report and in the 2022 Annual Progress report.

3. The development and operationalization of the PoCs directory will allow to collect best practices, and include valuable experiences from regional and sub-regional levels in setting up lines of communication to coordinate, and/or communicate in the event of significant cyber incidents.

4. It will be crucial to determine the specific objectives, as well as the operational role of the global PoCs Directory, also in view of ensuring complementarity and coordination with the already existing efforts by regional organizations on CBMs and regional initiatives to develop various PoCs directories on cyber security.

5. Let me offer you an overview on the existing confidence building PoCs initiatives in our European region. In 2013, as part of the initial set of CBMs, the OSCE established a network of national PoCs of participating states to facilitate pertinent communications and dialogue on security of and in the use of ICT. It was later

expanded to accommodate the crisis communication network. The same contact network can be also leveraged as a platform for broader co-operation in cyber security.

6. The OSCE cyber security PoCs list contains both policy experts from the MFAs and technical experts from national CERTs. The network can be accessed via a website only by dedicated staff at national delegations and OSCE Secretariat.

7. The OSCE has also emphasised the in-person meetings for PoCs, bilateral country visits, as well as small-scale crisis simulations. This has facilitated communication between States in the OSCE area and created more trust as well as common understanding on threat perceptions, approaches to cybersecurity capacities and strategic priorities.

8. Other regional organisations, such as the OAS and ASEAN Regional Forum have also developed their cyber confidence building mechanisms that suit the participants of their respective forums. We need to make sure that a new global PoC directory will integrate the regional best practices and serve as a complementary tool to existing regional initiatives.

9. Keeping in mind that not all States are members of regional organizations or of regional organizations' cyber confidence building initiatives, the global intergovernmental points of contact directory on security in the use of ICTs established under the UN auspices will benefit from clear guidance how to set up the contact network at technical and political levels.

10. The global directory should certainly build upon and complement the existing regional initiatives on PoCs Directories, enhance interaction and cooperation between States and bring in those states that have not been part of these efforts before.

11. We also have similar initiatives at the EU level in the area of crisis management, such as the Cyber Crisis Liaison Organization Network (CyCLONe) that was created in 2020 and is driven by the EU Member States. It brings together the agencies in charge of cyber crisis management of the 27 EU Member States both at technical (e.g. Computer Security Incident Response Team - CSIRTs) and political levels (e.g. Integrated Political Crisis Response - IPCR).

12. CyCLONe is enabling rapid cyber crisis management coordination in case of a large-scale cross-border cyber incident or crisis in the EU by providing timely information sharing and situational awareness amongst competent cyber authorities.

13. With the Network and Information Security (NIS) Directive, adopted on 6th of July 2016, we have also established the CSIRTs Network with the goal to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation in case of a major cyber incidents with cross-border effects.

14. These two platforms help to foster real-time exchange of information between the EU's cyber experts and create a trusted environment for informal exchanges between technical, operational and strategic levels. These communities also organize regular physical meetings for exercises and policy-related discussions, which is an important factor for building trust inside the EU's cyber eco-system.

15. Regular meetings of EU Member States' cyber ambassadors and coordinators are also brought together by the rotating Presidencies and the External Action Service to discuss strategic, political issues relevant to the EU's participation in international and bilateral cybersecurity negotiations and processes.

16. I hope that this small overview has offered some food for thought how the global UN PoC directory could be set up, and what are the other fora where to look for best practices. The EU will look forward to continuing these discussions with the UN Member States and regional organizations. Thank you very much for your support.