**Fourth Substantive Session of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025**
**Remarks of the Inter-American Committee against Terrorism**
**Organization of American States**

Chair, we would like to thank you for giving us the opportunity to take the floor and crave your indulgence as we have merged our brief comments on CBMs and the POC in this intervention given the relevance to the experiences we wished to share. We recognise that not all member states here are aware of the OAS and we wanted to provide some perspective on regional organizations such as the OAS should be encouraged to share their knowledge and experience unique to their region. And, as such we are grateful for the opportunity to do so today.

As such, we would like to highlight that the OAS member states have had a regional cybersecurity strategy since 2004 and have established a Cybersecurity Program which has been operational for over 18 years. As a result, today our region has made good and important advances, including the development of 20 national cybersecurity strategies, with five others under development; and over 10,000 public and private sector representatives benefitting from training in such areas as international law in cyberspace, technical training for youth; gender and cybersecurity, among others.

Further, this progress has included the establishment of a working group on Cyber CBMs, which has a list of 6 confidence-building measures to help guide Member State behavior in cyberspace, and include:

- Provide information on **cybersecurity policies**.
- Designate a **national cyber point of contact** at the policy level.
- Designate **points of contact** in the Ministries of Foreign Affairs.
- Develop and **strengthen capacities** through cyber diplomacy.
- Promote the incorporation of cyberspace and cybersecurity **training for diplomats**.
  Foster **cooperation and exchange of best practices** in cyber diplomacy, cybersecurity and cyberspace through the establishment of working groups

As some of our member states have alluded to, in our 4th CBMs Working Group Meeting, member states proposed five new CBMS touching on issues relevant to this OEWG and will be deliberated on for approval later this year. They include **Gender and the need to encourage** and promote the inclusion, leadership, and effective and meaningful participation of women in decision-making processes linked to information and communication, in line with the women, peace, and security agenda. The undertaking of research and the promotion of voluntary exchanges of positions and national vision statements, opinions, legislation, policies, and practices as it relates to the application of international law to the use of information and communications technologies in the context of international security. **Recognizing the need to harmonize with the UN processes, member states proposed as a CBM, the implementation of 11 voluntary, non-binding norms** and promote reporting on these efforts taking into account the national implementation survey. The promotion of dialogue with all stakeholders, including civil society, academia, the private sector, and the technical community, among others. Finally, it was recommended that

member states develop their own **national cyber incident severity schemas** and share information about them

Chair, it is important to highlight to member states here that in the case of the OAS, the OAS/CICTE is the dedicated Secretariat for the WG and is responsible for **maintenance of the list of PoC** for Working Group on Cooperation and Confidence-Building Measures in Cyberspace and Cyber related Policy and Legislation Repository, **provision of** updates on current issues related to the **applicability of international law to cyberspace, development of a web portal to manage the cyber policy points of contacts and policies and legislation related to cybersecurity, communication and organization of formal and informal meetings of the Working Group and Development of Reports and presentations on the progress of the working group and delivery of diplomacy courses which have benefitted over 31 countries and over 500 officials trained.**

**Currently, there are currently 97 policy points of contact, and 19 Ministry of Foreign Affairs contact from 30 countries. However, we wanted to highlight that as it relates to technical officials** – the OAS/CICTE manages the CSIRTs Americas Network, the only regional network linking together 36 CSIRTs from 21 countries with 221 cybersecurity specialists throughout the region, with 4 other CIRTs requesting adhesion. The Network is comprised of 19 national CSIRTs, 9 military CSIRTs and 8 local governmental CSIRTs. 74% of the cybersecurity specialists that are part of the Network are men, 25% are women and 1% prefer not to say. In leadership positions 31 (72%) are men and 12 (28%) are women. In addition, we would like to reference and acknowledge that at the global level there is the Forum of Incident Response and Security Teams (FIRST), which according to publicly available information has 683 Teams in 104 different countries, which represents both national and private sector CIRTs and can be explored as for harmonization should UN member states deem relevant.

Chair, there are several challenges that come with maintaining these directories such as the need to ensure security updates for the portal, frequency or lag in user log ins to the portal, funding to expand services within the portal and the frequent turnover of persons nominated as POC for various reasons.

Some activities we have found that works include, periodic reminders and facilitation of information on existing implemented measures, a dedicated technical team member to ensure monitoring of the network for security and stability purposes, content is up to date, and develop activities such as ping tests, webinars and national and subregional TTX around the Points of Contacts specifically.

Chair, the OAS sees the potential value of a Global POC directory for facilitating information exchange cross-regionally. We also know, however, of the significant technical and financial resources required to not only develop such a directory but to maintain it. We therefore would respectfully suggest that serious consideration be given to how these aspects would be addressed over the long term to ensure the directory's sustainability and effectiveness. The OAS would of course be happy to share more details about its own experiences with developing such a directory if that would be of service.

Thank you for the opportunity to address you today.