Statement by Derechos Digitales before the Open-Ended Working Group on security of and in the use of information and communications technologies (OEWG 2021-2025)

Informal intersessional session (5-9 December, 2022)

6 December 2022

Thank you, Mr Chair. Mr Chair, distinguished delegates,

Derechos Digitales wishes to express its gratitude for the opportunity to participate in this intersessional meeting of the Open-Ended Working Group, and we wish to make a statement on the subject of CBMs. We are a civil society organisation defending digital rights in Latin America, active in research, capacity building and exchange of information on threats in cyberspace.

We believe all confidence building measures can benefit from stronger participation by non-governmental stakeholders, including the private sector, the technical community, academia, and civil society organisations and human rights defenders. The involvement of civil society in the development of confidence-building measures can help not only to refine these measures, but also to encourage implementation of voluntary norms and CBMs and thus improve trust in governments.

We acknowledge the work at the Organisation of American States regarding specific CBMs in the Americas. Yet we urge for greater inclusion of non-governmental stakeholders in developing new CBMs as expressed by the OAS today, as diverse actors can help to identify the issues to be addressed and measures that can be useful to create trust in different contexts. Cooperation with state actors and other non-governmental stakeholders can help effectively implement these measures at the regional and local level.

On the issue of a global **Points of Contact Directory**, we also wish to support the possibility of expansion of this directory beyond state representatives to trusted key contacts from non-governmental stakeholders, such as academics, civil society, infrastructure operators and others with expertise in the response to cyber incidents and threat mitigation, as part of future discussions in this Working Group. We urge States to consider the available expertise outside of governments.

Moreover, we wish to highlight the role of non-governmental stakeholders in developing promoting standards for transparency and information exchange by States. As human rights defenders, we are concerned about the deployment of state capabilities for cyber attacks, as well as the lack of proper information exchange on vulnerabilities and threats that could affect other states, all data points that can be identified by civil society and non-state experts.

Finally, we encourage states to recognise the existing efforts to openly discuss the governance of digital spaces. Only last week, the **Internet Governance Forum** took place, a space for rich discussions in many topics related to security in cyberspace. These spaces can be promoted and fostered by states, to facilitate multiple stakeholder engagement, in a holistic and sustained manner. The establishment of opportunities for open, multi-stakeholder discussion is by itself a measure to build trust among all stakeholders in cyberspace, including States.

Thank you, Mr Chair.