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),
Fourth Substantive Session (6-10 March, 2023)

9 March, 2023– J. Carlos Lara Gálvez

Mr Chair, distinguished delegates,

Derechos Digitales is grateful for the opportunity to address this Working Group on the topic of capacity building. We are a human rights organisation focused on the impact of the use and regulation of digital technologies, and the effects of cyber threats in the enjoyment of all human rights and social justice in Latin America. These impacts are compounded when knowledge gaps limit effective prevention and mitigation of harm from those threats.

We concur that capacity building is essential to foster peace and security in cyberspace, and a condition for the effective operationalisation of agreed norms. We recognise the breadth of subjects where capacity and knowledge gaps may exist, and support proposals by States to allow further discussion and foster common understanding regarding many of the subjects discussed in this Working Group. Partnerships among States and non-governmental is key for the success of those efforts.

Derechos Digitales commends the efforts conducted by States, international organisations, and academics, to fund and organise formal training programmes, including those on cybersecurity and gender, and recognise the efforts to include expertise from members of the private sector, academia, and civil society.

But there is still complementarity with other contributions, including our own work. Derechos Digitales conducts, funds and supports the development of digital security trainings in Latin America, in partnership with local experts, directing efforts towards groups including women, LGBTQI+ individuals, indigenous groups, and others. We facilitate a nascent network of non-governmental organisations exchanging information on cyber threats, developing distributed capacities for threat response. We have collaborated in gender-sensitive trainings on cybersecurity by the police in Chile. And more examples abound.

We believe this experience, in substantive issues and in information exchange across countries and groups, is a fundamental source of knowledge to understand the lived experience of developing countries in the face of cyber threats, and can help identify the needs for further capacity-building efforts

Finally, we join recommendations to include, in the upcoming report of the Working Group, the recognition of the role of non-governmental stakeholders in capacity building efforts, and the integration of their expertise in all areas of capacity building, nationally and internationally, to operationalise the agreed framework.

In summary, cooperation in capacity building is by itself a means to breach knowledge gaps, as well as to enhance the role of capacity building to build an open, secure, stable, accessible, and peaceful cyberspace.

Thank you, Chair.