APC statement to the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security 2021-2025

Virtual Informal Dialogue with the Chair

3 July 2025

Delivered by Verónica Ferrari, APC Global Policy Advocacy Coordinator

Mr. Chair,

Distinguished delegates, colleagues,

APC welcomes the opportunity to engage in this informal dialogue.

We welcome the reference in the zero draft of the final report to the importance of engaging stakeholders in a “systematic, sustained and substantive manner”. Maintaining peace and stability in cyberspace is not the work of one actor, and governments can only address complex, global cyber threats collectively, with non-state actors. Groups in vulnerable situations and those affected by cyber operations need to be part of these discussions, as states continue discussions within the future permanent mechanism.

We also value the reference to the need for a gender perspective in addressing ICT threats to address the specific risks faced by persons in vulnerable situations. When exchanging views as part of the future mechanism, we encourage states to generate, in consultation with multistakeholder partners and especially civil society, gender-responsive definitions of cybersecurity, critical infrastructure and ICT threats.

This leads to the question of how stakeholders can work together with states in addressing these issues. In particular, civil society plays a key role in demonstrating the perspectives, experiences and realities of vulnerable groups by providing evidence and analysis based on the experiences of those who face cyber incidents. This can contribute to a better understanding of the actors involved, the form and the impact of these incidents.

Civil society can also support evidence-based, human-centric, rights-respecting approaches to norm implementation by developing working papers, guidance, capacity building and research.

Building on the OEWG discussions on the gender-differentiated effects of cyber threats and the need to develop gender-responsive cyber capacity building, we recommend the future permanent mechanism to incorporate an

explicit reference to gender equality. We will provide written comments with specific recommendations, but ways to integrate gender into the mechanism may include:

- Enabling meaningful and diverse stakeholder participation in the set-up of this mechanism and actively engaging them to define its purpose, scope, form and content. Stakeholder engagement should aim at geographical representation and gender parity, as expressed in the November 2024 non paper led by Canada and Chile.

- Including explicit references to human rights and gender equality as part of the aims of the future permanent mechanism and mainstreaming these approaches in the work of the dedicated thematic groups, review conferences, plenaries and reports.

- Articulating guidance on gender-responsive implementation of the norms and including gender-related questions in future reporting practices or templates, building on recent research supported and funded by the Organization of American States (OAS) and the United Nations Institute for Disarmament Research (UNIDIR).[1]

Thank you for your attention.

1 Millar, K., & Ferrari, V. (2025). *A Novel Approach to the 11 UN Norms for Responsible State Behaviour in Cyberspace: Guidelines for Gendered Implementation*. Organization of American States & UNIDIR.