A statement at the informal dialogue with interested stakeholders of the Chair of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security 2021-2025

21 July 2022

Delivered by Verónica Ferrari, APC Global Policy Advocacy Coordinator

Distinguished Chair, colleagues,

My name is Verónica Ferrari and speak on behalf of the Association for Progressive Communications (APC). APC is an international civil society organisation and a network of members dedicated to empowering people working for peace, human rights, development and protection of the environment, through the strategic use of digital technologies. APC supports women, gender-diverse people and vulnerable groups to safely connect and use digital technologies in ways that respond to their lived realities.

APC welcomes the opportunity to engage in this discussion.

In our intervention, we will focus on some aspects of the draft of the first annual progress report.

Firstly, we welcome the proposals in the draft to address existing and potential cyber threats. When further elaborating on these issues in future discussions, and building on the first OEWG final report, we reiterate our call for a human rights-based approach to existing and emerging threats to improve the security of people in all their diversity and to respond to their specific risks. We encourage the report to acknowledge that cyber threats and malicious cyber operations impact people differently, based on their access to power and resources.

1[www.apc.org](http://www.apc.org)
We also want to reiterate the importance of a gender-sensitive approach to cyber capacity building that was stressed by states across regions during the first OEWG discussions. A key outcome of the 2021 OEWG was the set of principles that should guide capacity-building initiatives. We reiterate our support of the principles that state that capacity building should respect human rights and should be gender-sensitive and inclusive, universal and non-discriminatory. We are glad to see gender considerations in this revised version of the draft.

A gender-sensitive approach to capacity building will allow re-evaluating the concept of cybersecurity to go beyond defence and threats, to have a better understanding of the complexities of security for women and groups in vulnerable situations. As we have said in the past, a gender perspective should be mainstreamed in capacity-building programmes. We also believe that these programmes should be developed inclusively and with full participation of women and people of diverse sexualities and gender expressions.

We support the recommendation in the draft progress report that calls for strengthening coordination and cooperation between states and non-governmental stakeholders, and the recognition that these actors are already playing an important role. For example, civil society organisations play a key role in bringing a human rights and gender perspective to national cybersecurity policies and strategies through research and support to policy makers, and developing training curricula tailored for women’s rights activists so they can use the internet safely, among other issues.

Finally, we want to reiterate that a human rights-based and a gender-sensitive approach to cybersecurity also means ensuring ample participation of multiple stakeholders in cyber discussions and empowering people for meaningful engagement in the design of cyber norms and policies.

Thank you for your attention and we look forward to continuing to engage in this process.