Delivered by Verónica Ferrari, APC Global Policy Advocacy Coordinator

Distinguished Chair, colleagues,

My name is Verónica Ferrari and I work with the Association for Progressive Communications (APC). APC is an international NGO and network of members working at the intersections of technology, human rights, and gender equality.

APC welcomes the opportunity to engage in this discussion.

In our intervention, firstly, we will focus on the question in the letter of the Chair related to the measures states can consider to address existing and potential cyber threats. We encourage states to further explore that what is considered a "threat" in cybersecurity has gendered implications.

Women and girls as well as people of diverse sexualities and gender
expressions are more often the targets of online violence. Increasingly, disinformation campaigns target these groups. And this situation is even more striking when applying an intersectional lens.

Even if these operations are not targeting people specifically on the basis of gender, they can have a more severe impact on these groups because of historical and structural inequalities.

As research by APC and the Women’s International League of Peace and Freedom (WILPF) shows, for example, internet shutdowns can create particular vulnerabilities for women in terms of personal safety, professional and economic development, emotional wellbeing, education, and connectivity. Data breaches can dramatically affect not only women and LGBTIQ+ people's privacy but also their health rights, their dignity and self-development.

Hence, and regarding possible cooperative measures, we encourage states to share good practices on how they incorporate gender considerations in their national cybersecurity policies and strategies. We would also like to support WILPF and Canada’s proposal on dedicating specific meetings to gender – for example, during the next OEWG meeting.

Regarding norms implementation, building on a recent report by APC, the Center for Internet and Society, Global Partners Digital and Research ICT Africa,¹ we reiterate that there is a need for greater adoption of existing norms. Furthermore the only long-term solution is regular dialogue and exchange, both between states and other stakeholders.

We encourage the group to develop mechanisms that promote learning of the already adopted norms, involving different stakeholders, to facilitate the sharing of experiences, including successes, challenges and lessons learned.

We also encourage further exploration of how the application of cyber norms can mitigate harm, especially to vulnerable communities.

Finally, we would like to reiterate the call for meaningful participation of civil society in this process. Civil society has been playing a key role in socialising the norms, supporting their implementation through research, and increasing capacity for understanding the norms and complying with them.

Meaningful engagement requires, among other things, easy and transparent access to information and the possibility, for both ECOSOC and non-ECOSOC organisations, to participate in all open meetings of the OEWG.

Any accreditation and registration process should be made clear and available in advance of meetings, to allow civil society adequate time to prepare.

We look forward to continue engaging in this process.

Thank you for your attention.