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

Delivered by Verónica Ferrari, APC Global Policy Advocacy Coordinator

APC STATEMENT
3 JULY 2024

Mr. Chair,

Distinguished delegates, colleagues,

APC welcomes the opportunity to engage in this informal dialogue and to reflect on how stakeholders, and in particular civil society, can work together with states to contribute to the implementation of the proposals in the Third Annual Progress Report (APR) of the OEWG.

Regarding Rules, Norms and Principles of Responsible State Behaviour, civil society supports the development and implementation of cyber norms by bringing expertise on human rights and gendered perspectives, and the differentiated impact that norms may have on different groups, especially marginalised communities. Civil society can work with states to ensure non-discrimination in the design and implementation of cyber norms.

Civil society also supports the implementation of norms at the national level, by leading capacity-building and awareness-raising efforts on the existing framework, documenting incidents and impacts of cyber threats, and running computer incident response centres. Civil society also contributes and engages in policy making at the national level, providing guidance for the development of national cybersecurity policies and strategies and developing practical recommendations on how to design inclusive policy-making processes.

Regarding Threats, we welcome the recognition of the prominence of the gender perspective in the Group discussions and the continued call for attention to the need for a gender perspective in addressing ICT threats and the specific risks faced by persons in vulnerable situations.

Overall, we welcome the increasing recognition of the fact that cybersecurity incidents affect genders differently. In support of these discussions, civil society can bring context-based research and evidence on how cybersecurity incidents affect genders differently and, for example, how women and gender-diverse individuals in the global South face specific circumstances and challenges related to cyber attacks. As APC research on gendered disinformation argues,[1] although these are global issues, there is also a need to understand and address cyber threats from regional and local perspectives. More research to bring attention to the realities of women, girls and gender non-conforming individuals in the global South is needed. We encourage states to engage with civil society for this.

[1] https://www.apc.org/en/project/placing-gendered-disinformation

In applying measures to increase the security and stability of ICT practices, civil society can partner with governments to understand “critical infrastructure” in ways that are human-centric and holistic.[2] Critical infrastructure risk models should incorporate a gender and intersectional approach to protecting the rights of people given their diverse needs. Governments can explore collaboration with civil society to coordinate training sessions with stakeholders on how the gender approach can contribute to developing these models and creating plans for timely responses to incidents.

Therefore, any future permanent mechanism for regular institutional dialogue should explicitly recognise the key role of civil society and that meaningful engagement of the multistakeholder community is key to promoting an open, secure, stable, accessible and peaceful ICT environment.

[2] https://www.apc.org/en/pubs/framework-developing-gender-responsive-cybersecurity-policy