OEWG Third Substantive Session: Key messages from the Association for Progressive Communications

July 2022

1. Introduction

The Association for Progressive Communications (APC)[1]1 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 to and use digital technologies in ways that respond to their lived realities.

We approach cybersecurity as a human rights issue since people are the ones impacted by cyber incidents and threats. We advocate for an approach to cybersecurity that puts a focus on the harm to people, addressing the differential impact of cyber incidents based on gender and other intersections. We also work to make cybersecurity processes more open, participatory and diverse. We conduct

[1] https://www.apc.org

research on these issues and monitor and engage in cyber policy development at global, regional and national levels.

We welcome the opportunity to submit our response to the third substantive session of the Open-Ended Working Group on the security of, and in the use of, information and communications technologies (OEWG). Our input addresses some of the recommended next steps outlined in the draft progress report[2] and the guiding questions for discussions with stakeholders from the Chair's letter of 22 June.

2. APC comments on the OEWG draft progress report

2.1. Existing and potential threats

We welcome the concrete and action-oriented proposals in the zero draft progress report to address existing and potential cyber threats.

When further elaborating on these issues in forthcoming OEWG sessions, and building on the first OEWG final report, we reiterate our call for a human rights-based approach to existing and emerging threats so that cybersecurity can improve the security of people in all their diversity and respond to their specific risks. The impact of cyber threats and malicious cyber operations affects people differently, based on their access to power and resources.

Cyber operations and attacks linked to conflict or tension between states cause harm to humans. A rights-based approach means, among other issues, putting a focus on the harm to humans, and recognising the differentiated impacts of cyber incidents based on gender and other intersections. These considerations should be an essential part of the ongoing process and the report could go further on this.

This approach also seeks to ensure that there is trust and security in networks and devices that reinforce, rather than threaten, human security. Transparency and participation are also critical elements of a rights-based approach to cybersecurity. We welcome the recommendations on the need to strengthen interactions with interested stakeholders, including civil society, through the exchange of knowledge and best practices on the protection of critical infrastructure (CI) and critical information infrastructure (CII). States' critical infrastructure risk models should incorporate human rights and a gender-sensitive approach to protecting the rights of people in their diverse needs. We encourage the OEWG to go further and involve all stakeholders for both implementation and development of measures to address and respond to cyber threats, and believe that this should be emphasised in the OEWG report.

[2] https://documents.unoda.org/wp-content/uploads/2022/07/Letter-from-the-OEWG-Chair-20-July-2022.pdf

2.2. Rules, norms and principles

We support the proposal related to states surveying or voluntarily reporting on their national implementation of rules, norms and principles of responsible state behaviour utilising existing avenues and tools such as the National Survey of Implementation, as contained in the recommendations of the 2021 OEWG report.

Moving forward, we emphasise again the role of all relevant stakeholders, including civil society, in supporting states' efforts to implement the agreed-upon norms.

Civil society plays a key role in cyber norms implementation, producing research, developing cyber capacity building and monitoring their implementation.

Civil society has experience working with states in monitoring United Nations system implementations. We support the OEWG recommendations for a voluntary non-binding state survey of national efforts to implement the norms. We believe, however, that mechanisms led by states with input from relevant stakeholders, through which voluntary assessment can be made in a more consistent manner, are needed. A voluntary state-led review process, involving multistakeholder participation to facilitate the sharing of experiences, including successes, challenges and lessons learned in implementing the norms, would help in making progress in achieving the goals represented by the norms.

2.3. International law

We welcome the recommendation that encourages states to continue exchanging views at the OEWG on how international law applies in the use of ICTs.

In these discussions going further, we encourage the OEWG to emphasise that protection of human rights is a security issue and international human rights law should be the guiding principle in maintaining a peaceful cyberspace.

A human rights-based approach to cybersecurity means, at a minimum, recognising international human rights law as the standard for a peaceful and stable cyberspace. States should comply with their international human rights obligations when designing and putting into place cybersecurity initiatives.

Discussions of the legal aspects of international peace and security and justice should integrate an understanding of the effect of malicious cyber operations on vulnerable groups.

2.4. Capacity building

We welcome the inclusion of language on the necessity to promote a better understanding of the needs of developing states with the aim of narrowing the digital divide. In the OEWG I, states such as Cameroon, South Africa and Kenya, among others, noted that digital divides are a threat in themselves. Gaps in terms of internet access and digital skills should be seen as security concerns since they are factors that create differential vulnerabilities to cyber attacks.

We also welcome a recommendation in the revised version of the draft to states to engage in focused discussions on the gender dimensions of ICT security and best practices on how to incorporate the gender dimension in ICT-related projects, including the collection and use of gender-disaggregated data to determine how gender is connected with participation. Gender biases and stereotypes are steering girls, women and people of diverse sexualities and gender expressions away from the cybersecurity field. We reiterate that diversity and participation are not only about numbers and percentages. Cybersecurity impacts everyone, and women and LGBTIQ+ people should have equal opportunities to participate in the decisions, policies and programmes that will affect them. And we also reaffirm that a gender-sensitive approach to cybersecurity is not only about participation.

We recall 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.

This was an important first step and we believe the future discussions at the OEWG should build on these principles and explore them further, in particular, the importance of gender-sensitive capacity building.

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 situations of marginalisation. A gender perspective should be mainstreamed in the design, implementation and evaluation of capacity-building programmes. We also believe that these programmes should be developed inclusively and with full participation of women's, LGBTIQ+ and racialised groups and communities, among others.

We support the recommendation in the zero draft progress report that calls for strengthening coordination and cooperation between states and interested non-governmental stakeholders and the recognition that these actors are already playing an important role through partnerships with states for the purposes of training public officials, research, and facilitating access to the internet and digital services. We also support the proposals on experts that could be invited to make presentations on these topics to facilitate further discussion.

Civil society and women's rights groups could enrich the OEWG discussions, for example, through their experience in bringing a human rights and gender perspective to national cybersecurity policies and strategies and in developing training curricula tailored for women's rights activists so they can use the internet safely, creatively and strategically.

2.5. Regular institutional dialogue

We welcome the recommendations to states to continue the discussions on the elaboration of a Programme of Action (PoA) for advancing responsible state behaviour in ICTs within the framework of the OEWG, and further discuss the relationship between the PoA and the OEWG and the scope, content and time frame for the establishment of a PoA.

We support the proposal of an inclusive, action-oriented UN Cyber Programme of Action that could help states implement the agreed cyber norms, coordinate capacity-building efforts and better integrate the voices of non-governmental actors.

As mentioned earlier, civil society plays a key role in cyber norms implementation, producing research, developing cyber capacity building and monitoring their implementation. The UN Cyber PoA should explicitly recognise the role of non-governmental actors and should incorporate gender and intersectional perspectives. It is also key to include non-state actors in continuing institutional dialogue and the design and implementation of the PoA.

We emphasise again the importance of recognising that maintaining peace and stability in cyberspace is a multistakeholder job. Only with non-state actors can governments and multilateral forums address complex and global cyber threats.

Groups in situations of marginalisation and those affected by cyber operations should be part of these discussions.

2.6. The need for an intersectional gender perspective in international cybersecurity

It has been encouraging to see in the OEWG a growing number of states from different regions calling for a gender-sensitive approach to international cybersecurity. The OEWG I adopted a final report that highlighted the participation of women delegates in the process and the importance of promoting meaningful participation and leadership of women in cyber policy-making spaces. The report acknowledged the importance of bridging the "gender digital divide" and recognised that people in positions of marginalisation or vulnerability experience particular cyber risks.

For APC, gender matters in international cybersecurity since it shapes and influences our online behaviour, determines access and power, and is a factor in vulnerability.

An intersectional gender perspective recognises that numerous factors, among which is gender but also race, ethnicity, religion, social class, among others, can intensify the experiences of people affected by cyber operations.

We saw with regret that language on gender was absent from the zero draft progress report and we welcome the inclusion of gender references in the revised version. We strongly encourage the OEWG to recognise that gender considerations should be integral to the different areas of work of the group.

3. Guiding questions for discussions with stakeholders at the third substantive session of the OEWG

What are the various ways in which stakeholders are currently involved in supporting and/or delivering capacity-building initiatives in the context of the current ICT security capacity-building landscape?

Cyber capacity building comprises a wide range of activities including the development of national cyber strategies and policies, the sharing of good practices and lessons learned, and research that seeks to support policy-making processes. Civil society also conducts training on digital security tailored for specific needs and contexts. Civil society organisations also have an important role in making sure that cyber capacity building is informed by gender and human rights perspectives, following one of the capacity-building guiding principles in the previous OEWG final report. Below we present some initiatives led by APC that show the different ways in which civil society can contribute to:

- Human rights and gender perspectives in national cybersecurity policies: Civil society organisations play a key role in bringing a human rights and gender perspective to national cybersecurity policies and strategies. APC is now conducting research on how to better incorporate a gender perspective in cybersecurity national policies and will soon launch a framework to assist national policy makers in doing that.
- APC's Feminist Tech Exchange (FTX) develops training curricula tailored for women's rights activists so they can use the internet safely, creatively and strategically.[3] FTX's analysis and approach are framed by the Feminist Principles of the Internet (FPIs),[4] a set of principles which work towards empowering more women and queer persons to dismantle patriarchy and realise a feminist internet. In 2018 FTX collaborated with partners to develop the FTX: Safety Reboot,[5] a training curriculum made up of several modules for trainers who work with women's rights and sexual rights activists to use the internet safely, creatively and strategically. This initiative seeks to be a feminist contribution to the global response to digital security capacity building and enables trainers to work with communities to engage technology with pleasure, creativity and curiosity.
- The African School on Internet Governance (AfriSIG) is another APC capacity-building initiative. AfriSIG is an annual course whose goal is to strengthen the capacities of African leaders from diverse sectors and backgrounds to participate in local and international internet governance discussions. AfriSIG is designed, developed and run by colleagues in and from the region, together with partners like the African Union, Research ICT Africa and Global Partners Digital. This focus of this year's AfriSIG was international cybersecurity.[6]

[3] https://www.apc.org/en/project/feminist-tech-exchange

[4] https://feministinternet.org

[5] https://en.ftx.apc.org/shelves/ftx-safety-reboot

[6] https://afrisig.org/afrisig-2022

- The Take Back the Tech! campaign[7] is a global, collaborative campaign project initiated by APC in 2006 that highlights the problem of tech-related violence against women, together with research and solutions from different parts of the world. The campaign offers safety roadmaps and information and provides an avenue for taking action. Take Back the Tech! leads several initiatives at various points in the year, but its biggest annual campaign takes place during the 16 Days of Activism Against Gender-Based Violence from 25 November to 10 December.

[7] https://takebackthetech.net