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

Capacity-building mapping exercise

The Association for Progressive Communications (APC)[1] is an international civil society organisation and a network of members dedicated to empowering and supporting people working for peace, human rights, and development and protection of the environment through the strategic use of digital technologies (ICTs). APC has 62 organisational members and 41 associates active in 74 countries, mostly in the global South.

APC promotes a human rights-based approach to cybersecurity since humans are the ones impacted by cyberthreats, incidents and operations. We also apply a gender approach to cybersecurity, recognising that cyberthreats differentially affect groups in positions of marginalisation or vulnerability because of their sexual orientation or gender identity.[2]

APC conducts research on cybersecurity and monitors policy development on this topic at global, regional and national levels. We work collaboratively with our members, partners, other civil society organisations, academia and the tech community to advocate for the development of principles and norms to promote the idea of a rights-based approach to cybersecurity. APC also maps policies in its members' countries and regions. At the global, regional and national levels, APC advocates for more open and participatory cyber policy processes.

APC has been following and contributing to the United Nations General Assembly's First Committee's Open-ended Working Group (OEWG) on the security of, and in the use of, ICTs since the inception of the group. We welcome the opportunity to submit our inputs to the OEWG mapping on the landscape of ICTs' capacity-building programmes and initiatives at the global and regional levels.

[1] www.apc.org
[2] https://www.apc.org/es/node/36999

Capacity-building in the context of cyberspace –or cyber capacity building (CCB) – can cover a wide range of efforts including cybersecurity policy, cybercrime law enforcement capacity, and cybersecurity culture, awareness and skills, among others.[3]

All relevant stakeholders play a key role in CCB and there is a need for coordination and cooperation between states and interested non-governmental stakeholders. In particular, civil society organisations play in key role in training and convening stakeholders in producing research that helps to build capacity on cybersecurity, bringing human rights and gender perspective to national policies and strategies, developing training curriculums tailored for women's rights activists so they can use the internet safely, and implementing capacity-building initiatives sensitive to local and regional contexts. In this submission, we present initiatives led by APC related to these CCB areas.

Cybersecurity policy

Guidance on integrating gender into national cyber legislation and strategies

Building on its research and advocacy work, APC develops tools to support the work of different stakeholders in cybersecurity policy. For example, APC put together *A framework for developing gender-responsive cybersecurity policy*[4] to support policymakers and civil society organisations in achieving gender-responsive cybersecurity policies and strategies.

A gender approach to cybersecurity is a fundamental tool for policy that focuses on the human rights of people in cyberspace. But, most notably, it is a perspective that seeks to make cybersecurity responsive to the complex and differentiated needs of people when systems of oppression based on factors such as gender, sexual orientation, race, ethnicity, ability and class, among others, intersect.

This framework is made up of:

- A document identifying norms, standards and guidelines that cybersecurity policymakers and advocates can draw on when seeking to promote a gender approach within national or multilateral cybersecurity discussions.
- A literature review that explores how cybersecurity as a gendered space has been addressed in research.
- An assessment tool that provides recommendations to develop a gender approach to

[3] https://www.gp-digital.org/wp-content/uploads/2019/10/RSB-1_CCB_export__FINAL.pdf
[4] https://www.apc.org/en/pubs/framework-gender-cybersec

cybersecurity policy that provides practical guidance for developing gender-responsive cybersecurity policies, laws and strategies, by offering concrete recommendations so that stakeholders can find inspiration to help deploy the transformative power of a gender perspective in cybersecurity, depending on the stage of maturity of national policies in each country.

Enhancing regional stakeholder capacity for global policy engagement

APC has been organizing training activities to equip stakeholders with the capacities needed to engage in global cybersecurity policy discussions. For example, the African School on Internet Governance (AfriSIG) is an annual initiative whose goal is to strengthen the capacities of African leaders from diverse sectors, backgrounds and ages with the skills to participate in local and international internet governance discussions.

AfriSIG is a joint initiative of APC, the Information Society division of the African Union Commission (AUC) and Research ICT Africa. AfriSIG provides a cutting-edge and African-centred curriculum, designed so it responds to local and regional contexts and needs. AfriSIG provides exposure to and hands-on experience in participating in internet governance mechanisms, besides extending ongoing mentorship to students. Alumni are also plugged into a rich network of policymakers, regulators, rights activists and experts invested in realising an open and secure internet.

The 10th edition of AfriSIG in 2022,[5] in which APC partnered with Global Partners Digital, was focused on international cybersecurity and capacity-building needs in Africa. AfriSIG 2022 gathered existing and emerging leaders from all stakeholder groups in the field of international cybersecurity. This edition aimed at feeding the OEWG discussions brought together participants from governments, civil society, business, the technical community, the media and other relevant stakeholder groups who are already participating in international cybersecurity debates from an African perspective.[6] The discussions held during this edition of AfriSIG were prominently featured during OEWG sessions, and the conclusions reached were incorporated into statements and contributions made to the group.

Cybersecurity awareness and skills

Awareness-raising and CCB activities connected with digital security are essential for a safe internet. APC develops tailored trainings for women’s rights activists so they can use the internet

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

[6] https://www.apc.org/en/news/afrisig-2022-strengthening-african-capacity-and-participation-international-cybersecurity

safely. One such training is the Feminist Tech Exchange (FTX)[7], which seeks to be a feminist contribution to the global response to digital security capacity building.

FTX brings a unique methodology and approach to cyber capacity building (CCB). FTX creates safe, creative and feminist spaces of exchange and experience where the politics and practice of technology are informed by local and contextual realities of women, and build collective knowledge and ownership.

FTX was developed in response to the expressed needs of feminist and women's rights movements for greater understanding of emerging internet and technology-related issues, trends, governance and application in feminist activism. FTX facilitates inter-movement building between women's rights activists, LGBTQIA+ movements, internet and technology rights organisations, and human rights advocates.

APC emphasises local ownership of FTX, and since 2008, when we hosted our first FTX in partnership with the Association for Women's Rights in Development (AWID) and trained over 100 women, we have seen the uptake of FTX by our members and partners in many countries and regions and at subsequent AWID Forums. Using an approach that prioritises feminist perspectives, women's rights and movement building, FTX:

- Builds capacity within feminist and women's rights movements in the creative and strategic use of information and communications technology (ICT).
- Supports the development of a community of trainers who can continue to augment the knowledge and skills of women's rights campaigners, and LGBTQIA+ and feminist advocates in different locales, advocacy areas and movements.
- Creates partnerships between feminist, internet rights and women's rights movements to sustain movement building as a space for open discussions and convergence between internet rights and women's rights agendas.
- Creates spaces where feminist politics and practices of technology are explored and discussed.

FTX analysis and approach are framed by the Feminist Principles of the Internet (FPIs),[8] a set of principles which work towards empowering more women and queer persons to dismantle patriarchy and realise a feminist internet. FTX methodologies encourage inclusivity, active listening and participation, and ensure that language diversity is respected and addressed in meaningful ways.

[7] https://www.apc.org/en/project/feminist-tech-exchange
[8] https://feministinternet.org/en

In 2018, APC collaborated with our partners to develop the FTX: Safety Reboot,[9] 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. It enables trainers to work with communities to engage technology with pleasure, creativity and curiosity. In 2019, APC hosted the FTX Convening,[10] which brought together feminist practitioners and trainers working on digital safety and self-care to share experiences on using the *FTX: Safety Reboot* curriculum and to inaugurate a network of trainers for ongoing support, advice and active solidarity.

The FTX Convening resulted in FTX small grants, which facilitated a range of impactful initiatives. These grants supported activities such as:

1. Training feminist activists in emergency response in Brazil.
2. Developing podcasts featuring conversations with feminist digital security trainers in Kenya.
3. Creating spaces and opportunities for women and gender non-conforming individuals to share their experiences in technology and holistic security in Puebla and Tlaxcala, Mexico.
4. Establishing a learning community for women freelance journalists in the same country, focusing on digital security practices and strategies to combat online gender-based violence (OGBV) using the FTX curriculum in Mexico.

The Take Back the Tech! Campaign[11], a global, collaborative campaign project initiated by APC in 2006 is another example of capacity building activity that seeks to raise awareness and highlight 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 campaigns at various points in the year, but the biggest annual campaign takes place during 16 Days of Activism Against Gender-Based Violence from 25 November to 10 December.

Enhancing capacity on the gendered impacts of cybercrime policy

The development and implementation of cybercrime legislation and the training of law enforcement agencies, the judiciary, the police and prosecutors to combat cybercrime is an important component of CCB. "The definition of what is and isn't permissible online, and what constitutes criminal activity – particularly with regard to content – has strong implications for freedom of expression, privacy, assembly, association, and other rights. Training subsequently has direct impact on the enforcement and legal interpretations of the legislation as well as the right to

[9] https://ftx.apc.org/shelves/multi-ftx-safety-reboot-all-languages
[10] https://genderit.org/edition/technology-feminist-creativity-and-care
[11] https://takebackthetech.net/

effective remedy. Equally, a lack of legislation, enforcement capacity and cross-border cooperation can leave individuals at increased risk."[12]

APC research has identified that as policymakers are called upon to respond to cybercrime challenges, it becomes critical to consider how cybercrime and cybercrime legislation have an impact on the social, economic and political participation of women and other marginalised groups.[13] Thus, it is important that everyone responsible for developing and strengthening the skills, abilities and resources of organisations and communities to survive and thrive in cyberspace – and those who support them – does so with due regard for gender equity and sensitivity.[14]

Several different types of conduct that generate harm on the internet have been classified as "cybercrime" by national laws, mainly because they occur in online spaces or because they are committed through the use of technology. In some cases, as will be seen below, acts that constitute online gender-based violence (OGBV) are included within these legislations. Cybercrime laws, however, normally refer to non-gender-specific acts or are designed without due consideration to gender inequalities. Criminal definitions are drafted in a broad manner and without applying a gender perspective in their formulation and implementation. As a result, the impact of the criminalisation generated by these laws also has specific effects on gender equality.

Laws created with the aim of combating OGBV, for example, are used to legitimise disproportionate censorship and surveillance measures, and in some cases are even used against those who invoke them for their protection. In turn, laws used to allegedly restrict disinformation are used to silence dissent, and national security and public order are invoked to initiate criminal prosecutions based on ill-defined offences in cybercrime legislation that often end up being used to repress dissent and control the online space, and "as a pretext to push back against the new digital civil society."[15]

APC teamed up with its Chilean member Derechos Digitales to produce research and recommendations that could enhance the capacity of policymakers with regard to the gendered impacts of cybercrime legislation. This research aimed at contributing to ongoing and future discussions concerning gender and cybercrime by providing concrete evidence of how national cybercrime laws have been used to silence and criminalise women and LGBTQIA+ people around the world.[16]

This mapping found that, although TFGBV (technology-facilitated, gender-based violence) is a serious and urgent concern, the use of criminal legislation to address it may create even further problems and this is the case, for example, of cybercrime norms. According to this research,

[12] https://www.gp-digital.org/wp-content/uploads/2019/10/RSB-1_CCB_export__FINAL.pdf

[13] Xu, W. (2010, 2 June). Unequal protection, cyber crime and the internet in India. *GenderIT.org*. https://genderit.org/articles/unequal-protection-cyber-crime-and-internet-india

[14] Chatham House. (2023, 5 July). Integrating gender in cybercrime capacity-building. https://www.chathamhouse.org/2023/07/integrating-gender-cybercrime-capacity-building

[15] Voule, C. N. (2019). *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*. A/HRC/41/41. https://undocs.org/A/HRC/41/41

[16] Derechos Digitales and Association for Progressive Communications. (2023, 26 October). When protection becomes an excuse for criminalisation: Gender considerations on cybercrime frameworks. https://www.apc.org/en/pubs/when-protection-becomes-excuse-criminalisation-gender-considerations-cybercrime-frameworks

"cybercrime laws tend to be open to abuse due to their vague terminology and lack of sufficient redress mechanisms. They are also not specifically tailored to address gender concerns."

Key recommendations include a call for strong cybersecurity strategies that put people and gender at the centre of public policies and actions as important responses to TFGBV as well as an important alternative to the use of cybercrime norms, which should be narrowly applied and interpreted.

Specific gender impact assessments should be carried out before any discussions on a bill on cybercrime take place in countries that do not have cybercrime legislation. For countries that have such legislation, it is important that the regulations be analysed from a gender perspective to enable the necessary changes to be made on the basis of these considerations. It is crucial to question the need for and potential effectiveness of cybercrime norms and refrain from using vague and overly broad terms in criminal definitions.

Gender-sensitive approach to capacity building

We want to recall in this submission the importance of a gender-sensitive approach to cyber capacity building (CCB) that was stressed by states across regions during OEWG discussions. We reiterate our support to the 2021 OEWG set of principles that should guide capacity-building initiatives that states that the latter should respect human rights, be gender sensitive and inclusive, universal and non-discriminatory.

A gender-sensitive approach to CCB recognises and responds to the differential cyber and critical tech access, opportunities, resources, benefits and risks to women and LGBTQIA+ and gender-diverse people. Unlike the traditional concept of cybersecurity, this approach avoids the assumption that everyone has the same needs, priorities and capacities related to cybersecurity.[17]

A gender-sensitive approach to CCB allows for the re-evaluation of the concept of cybersecurity to go beyond defence and threats, in order to have a better understanding of the complexities of security for women and groups in vulnerable situations.

This approach also ensures principles such as transparency, diversity and accountability, and encourages the participation of women and LGBTQIA+ people in projects, activities, approaches and outcomes, and empowers them with various resources so that they can fully engage. Therefore, a gender-sensitive approach should be mainstreamed in the development, implementation and evaluation of capacity-building programmes – not just added to existing programmes – and should allow the rethinking of cybersecurity education methodologies for all stakeholders.

[17] https://www.apc.org/en/pubs/apc-policy-explainer-what-gender-sensitive-approach-cyber-capacity-building#:~:text=Definition,sexualities%2C%20gender%20expressions%20and%20identities