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

Input to the zero draft of the final report and recommendations for the Open-Ended Action-Oriented Permanent Mechanism on ICT security in the context of international security

---

About APC: The Association for Progressive Communications (APC) is an international civil society organisation and a network of members dedicated to empowering and supporting people working for peace, human rights, development and the protection of the environment, through the strategic use of digital technologies. APC has 70 organisational members and 41 associates who are active in 74 countries, mostly in the Global South. We have been contributing to the UN General Assembly's First Committee's Open-ended Working Group (OEWG) on the security of, and in the use of, information and communications technologies since the group's inception.

www.apc.org

June 2025

1. Introduction

APC promotes a human rights-based approach to cybersecurity as it is humans who are impacted by cyberthreats, cyber incidents and operations. We apply an intersectional gender approach to cybersecurity, recognising that cyberthreats differentially affect groups which are marginalised or vulnerable because of their sexual orientation or gender identity.[1] Building on our research and advocacy work, we develop tools to support the work of different stakeholders in cybersecurity policy.[2] This input builds on our work in cybersecurity and on the research conducted in the context of developing a framework for integrating gender into the interpretation and implementation of the 11 UN norms supported and funded by the Organization of American States (OAS) and the United Nations Institute for Disarmament Research (UNIDIR). The research was co-authored by Verónica Ferrari, APC's global policy advocacy coordinator, and Dr Katharine Millar, associate professor at the London School of Economics.[3] The views and conclusions expressed in this submission are solely those of the authors.

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

[2] For example, APC has developed *A framework for developing gender-responsive cybersecurity policy* to support policy makers and civil society organisations to achieve gender-responsive cybersecurity policies and strategies. https://www.apc.org/en/pubs/framework-developing-gender-responsive-cybersecurity-policy#norms

[3] Millar, K., & Ferrari (2025). *A Novel Approach to the 11 UN Norms for Responsible State Behaviour in Cyberspace: Guidelines for Gendered Implementation*. Organization of American States, UNIDIR. https://unidir.org/wpcontent/uploads/2025/05/UNIDIR_Novel_Approach_11_UN_Norms_Responsible_State_Behaviour_Cyberspace_Guidelines_Gendered_Implementation.pdf

2. Comments on the zero draft of the final report[4]

A. Overview

Paragraph 10: We welcome the reference to the importance of engaging stakeholders in a "systematic, sustained and substantive manner". Maintaining peace and stability in cyberspace is not the work of one actor and governments can only address complex, global cyberthreats collectively, with non-state actors. Groups in vulnerable situations and those affected by cyber operations need to be part of these discussions, as states continue discussions at the future permanent mechanism.

Paragraph 12: We commend the recognition of the increasing participation of women delegates in the OEWG and the prominence of a gender perspective in its discussions. We also encourage the final report to continue underscoring the importance of narrowing the "gender digital divide". Gaps in internet access and digital skills are security concerns since they create differential vulnerabilities to cyber attacks. We also commend the reaffirmation of the need to continue promoting the full, equal and meaningful participation and leadership of women in decision-making processes related to the use of information and communication technologies (ICTs) in the context of international security. Cybersecurity impacts everyone, and women and LGBT+ people should have equal opportunities to participate in the decisions, policies and programmes that affect them.

B. Existing and potential threats

Paragraph 23: Considering the concerns expressed by states regarding the exploitation of ICT product vulnerabilities, the use of harmful hidden functions that impact international peace and security and the ICT threat posed to the integrity of supply chains, we encourage states to incorporate gender considerations into existing counter-proliferation measures (such as export licensing and arms control regimes) and ICT supply chain security governance processes, as they continue exchanging views at the future permanent mechanism on existing and potential threats. States can also discuss the development of measures to hold non-state actors accountable, including those

[4] UN OEWG, (2025). *Zero draft of the Final Report of the 2021-2025 UN OEWG*.

engaging in technology-facilitated gender-based violence (TFGBV), following human rights standards and due process.

Paragraph 24: Given the concerns expressed by states over ransomware attacks targeting critical infrastructure (CI) and critical information infrastructure (CII), we support the reference to the need for a human-centric approach to ransomware, to allow countries to better understand and mitigate its differentiated effects. Research has provided empirical evidence of the human and gendered impacts of this type of operation. For example, personal data breaches affect not only the privacy of women and people of diverse gender identities, expressions and sexualities, but also their sexual and reproductive health rights, dignity and self development.[5] Not using an intersectional gender perspective when defining and protecting critical infrastructure can exacerbate gender inequality. As states continue to exchange views on ICT threats at the future permanent mechanism, we commend them to discuss, with input from stakeholders, a gendered understanding of CI.

Paragraph 30: We value the reference to the need for a gender perspective in addressing ICT threats, to the specific risks faced by persons in vulnerable situations, and to the acknowledgment that the benefits of digital technology are not enjoyed equally by all, as well as the need to pay attention to the growing digital divide. When exchanging views on the future mechanism, we encourage states to generate, in consultation with multistakeholder partners and especially civil society, context-specific gender-responsive operational definitions of cybersecurity, CI and ICT threats. We encourage states to do this from an intersectional perspective, examining how gender relates to other dynamics of social marginalisation and disadvantage.

C. Rules, norms and principles of responsible state behaviour

Paragraphs 34 and 35: Given the discussions on rules, norms and principles, and the reaffirmation of the cumulative and evolving framework for responsible state behaviour in the use of ICTs, we note that the implementation of the norms is an ongoing and

[5] Pytlak, A. & Brown, D. (2020). *Why Gender Matters in Cybersecurity.* Association for Progressive Communications, Women's International League for Peace and Freedom. https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf
Shires. J., Hassib, B. & Swali, A. (2024) Gendered Hate Speech, Data Breach, and State Overreach. *Chatham House*. https://www.chathamhouse.org/2024/05/gendered-hate-speech-data-breach-and-state-overreach

dynamic process. In this context, we encourage states to build on the proposals developed in our recent report on gender and the 11 UN norms[6] at the future mechanism. The report proposes a human-centred, gender-responsive approach to the UN norms, to strengthen their implementation and, thereby, the security and stability of international cyberspace. Please find a summary with recommendations for gender-responsive implementation of each of the 11 UN Norms in Annex 1 of this submission.

Paragraph 37: We encourage states to integrate gender perspectives into the voluntary checklist of practical actions for the implementation of the norms. This would involve, for instance, adding a specific question about the gender equality implications of norm interpretation and implementation to the future mechanism discussions. It would also include gender mainstreaming the specific actions in the checklist in alignment with the recommendations in the report.

D. International law

Paragraph 39a: We are pleased that this paragraph reaffirms the recommendation of the first annual progress report of this OEWG, that states engage in focused discussions on topics including respect for human rights and fundamental freedoms. We further encourage states to discuss gender equality, recognising that, for effective cybersecurity, human rights and gender equality are mutually reinforcing.

Paragraph 41a: As discussions continue, we recommend the inclusion of experts in human rights, gender and sexuality equality as expert briefings are organised, with attention to geographical diversity and national contexts.

Paragraph 41d(iii): When strengthening collaborations with academics, civil society and the private sector to tailor international law capacity-building programmes, we encourage states to engage with human rights, digital rights and gender and sexuality equality civil society organisations.

Paragraph 42: We welcome the recommendation that encourages states to continue exchanging views at the OEWG on how international law applies in the use of ICTs. We encourage states to emphasise that the protection of human rights is a security issue and international human rights law should be the guiding principle in maintaining a

[6] Millar, K., & Ferrari, V. (2025). Op. cit.

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 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.[7]

Paragraph 43. We recommend this paragraph to encourage states to engage with non-government stakeholders when developing national positions on international law.

E. Confidence-building measures

Paragraph 46: As states continue their discussions at the future permanent mechanism on the development and implementation of confidence building measures (CBMs), including on the potential development of additional measures, we encourage them to mainstream talk around gender. For instance, states can:

- Foster dialogue through consultation and engagement with multiple stakeholders, facilitating consultations with a focus on gender equality and diversity[6] as proposed by a cross-regional group of states,
- Exchange views and undertake dialogue and consultations on perceptions of gendered experiences of threats and vulnerabilities, and related best practices; share their national efforts to incorporate gender perspectives into cybersecurity policies; and their efforts towards gender-responsive cyber-capacity building.
- Engage in the regular organisation of training programmes on ICT security with inclusive representation of stakeholders such as civil society organisations working on the rights of women andLGBT+ representatives.
- Exchange good practices and information related to the development of gender-responsive emergency plans for cyber incidents/critical infrastructure attacks.
- Consider the development of a specific CBM related to gender equality.
- Prioritise gender equality, through both women's participation and the application of a gender perspective, in cyber capacity building, following the OEWG's principles-based approach.

[7] APC. (2022, 25 July). OEWG third substantive session: Key messages from the Association for Progressive Communications. https://www.apc.org/en/pubs/oewg-third-substantive-session-key-messages-association-progressive-communications

F. Capacity building

Paragraph 51: We welcome that states will continue discussions on ICT capacity building by sharing national, regional and global experiences on ICT capacity building. We welcome the draft recalling and reaffirming the ICT security capacity-building principles adopted in the 2021 OEWG report and the continued emphasis on the need for further efforts to mainstream these principles into relevant capacity-building programming. We welcome the call for states to continue encouraging efforts to promote gender-responsive capacity building. The integration of a gender perspective into national ICT and capacity-building policies is also encouraged, as well as the development of checklists or questionnaires to identify needs and gaps in this area.

A gender-responsive approach to cyber capacity building recognises and responds to the differential cyber and critical tech access, opportunities, resources, benefits and risks of women and LGBT+ 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.[8] This approach also ensures principles such as transparency, diversity and accountability. It encourages the participation of women and LGBT+ people in projects, activities, approaches and outcomes, and empowers them with various resources so that they can fully engage. A gender-responsive approach should therefore be mainstreamed in the development, implementation and evaluation of capacity-building programmes – not just added to existing programmes. This would also involve developing capacity and expertise in gender-responsive cybersecurity practice and policymaking itself.

Paragraph 52: Regarding the recommendations on the discussions of capacity building at the future permanent mechanism, we recommend the following:

- Prioritise closing the gender digital divide and digital skills gap
    - Align cybersecurity capacity-building efforts with the activities of related UN agencies, alongside the Women Peace and Security (WPS) agenda
    - Address structural and systematic barriers to meaningful participation; provide safe and affordable digital connectivity for all women and girls; provide

[8] APC. (2023, 30 June). APC policy explainer: What is a gender-sensitive approach to cyber capacity building? https://www.apc.org/en/pubs/apc-policy-explainer-what-gender-sensitive-approach-cyber-capacity-building

opportunities for quality and inclusive STEM education and research; and promote women's and girls' participation in all roles and at all levels.

- Support women's, LGBT+ and other human rights organisations, as well as marginalised and minority communities, allowing them to develop the capacity to independently participate in cybersecurity governance processes with funding and access.
- Sustain, fund and strengthen technical and policy capacity-building efforts which specifically support women and people of diverse gender identities, expressions and sexualities to access cyber careers, informed by the OEWG's principles-based approach to capacity building.
- Promote inclusive cybersecurity capacity building through regular training and information sharing on gender-responsive emergency plans.

G. Regular institutional dialogue

Paragraph 62: We welcome the commitment to establish an action-oriented future permanent mechanism. We support the proposal of an inclusive mechanism that could help states implement the agreed cyber norms, coordinate capacity-building efforts and better integrate the voices of non-governmental actors.

3. General recommendations for the Open-Ended Action-Oriented Permanent Mechanism on ICT security in the context of international security

We encourage the future mechanism to explicitly recognise the key role of non-governmental actors across all the pillars of the framework for responsible state behaviour in the use of ICTs.

As previously expressed,[9] we underline the importance of broad representation and geographical diversity when organising briefings with relevant experts to discuss the impact of technologies in the context of international cybersecurity.[10] We encourage the future mechanism to engage with experts in human rights, gender and digital rights. Particular attention is required to ensure the participation and input of groups experiencing specific threats in cyberspace, such as human rights defenders, journalists, and people in marginalised or vulnerable situations.

Civil society plays a key role in demonstrating the perspectives, experiences and realities of these groups by providing evidence and analysis based on the lived experiences of those who face cyber incidents. This contributes to a better understanding of the actors involved, the form and the impact of these incidents.[11] Civil society also ensures evidence-based, human-centric, rights-respecting approaches to norm implementation by means of e.g. developing working papers, guidance and checklists to allow better understanding of key terms, contextualising the norms in national and local contexts.[12]

In addition, civil society contributes to overcoming challenges in the implementation of the UN norms, socialising them through capacity building and research. This includes

[9] APC. (2023, 26 July). APC statement at the dedicated stakeholder session at the fifth substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security 2021-2025. https://www.apc.org/en/pubs/apc-statement-dedicated-stakeholder-session-fifth-substantive-session-open-ended-working-group

[10] UN OEWG. (2025). *Draft Final Report, Zero Draft*. Annex III, paragraph 7.

[11] Fundación Karisma. (2024, 3 June). Ciberataque a Sanitas: Impactos Diferenciales Sobre Mujeres Cuidadoras. *Fundación Karisma.* https://web.karisma.org.co/ciberataque-a-sanitas-impactos-diferenciales-sobre-mujeres-cuidadoras/

[12] https://www.apc.org/sites/default/files/joint-civil-society-input-to-oewg-on-icts-draft-annual-progress-report.pdf

coordinating and convening other stakeholders[13] to increase awareness and capacity on the norms; providing oversight and accountability for norm transgression, etc. Organisations, especiallymainly those from the Global South, are also key to raising attention, e.g. to the inequalities in access to technologies. Civil society is active in a wide range of cyber capacity-building efforts: from developing tailored trainings so human rights defenders can use the internet safely, to awareness raising campaigns, to developing guidance on how to integrate human rights and gender into national cybersecurity laws and strategies.[14]

Finally, we encourage the future mechanism to incorporate explicit reference to gender equality. Recommendations for integrating gender into the future mechanism might include:

- Enabling meaningful and diverse stakeholder participation, including women's and LGBT+ organisations, in the set-up of this mechanism and actively engaging them to define its purpose, scope, form, and content. Stakeholder engagement should aim at geographical representation and gender parity, as expressed in the November 2024 non paper "Enabling stakeholders to add value to state-led discussions".[15]
- Including explicit references to human rights and gender equality as part of the aims of the future permanent mechanism and mainstreaming these approaches in the work of the dedicated thematic groups, review conferences, plenaries and reports.
- Building on the OEWG discussions on the gender-differentiated effects of cyber threats and the need to develop gender-responsive cyber capacity building, as part of the mechanism's substantive agenda.

[13] Joint civil society feedback on the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security revised non-paper norms proposals. https://www.apc.org/sites/default/files/joint-civil-society-groups-feedback-on-oewg-norms-proposals.pdf

[14] APC. (2022, 28 July). OEWG: APC emphasises key role played by civil society in cybersecurity capacity building. https://www.apc.org/en/pubs/oewg-apc-emphasises-key-role-played-civil-society-cybersecurity-capacity-building

[15] https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Enabling_Stakeholders_to_Add_Value_to_State-led_Discussions_in_the_Future_UN_Mechanism_for_Security_in_Cyberspace_-_Canada_and_Chile_Non_Paper_-

- Articulating guidance on gender-responsive implementation of the norms, building on the recommendations and actions outlined in the cited report and including gender-related questions in future reporting practices or templates.[16]
- Mainstreaming gender and intersectional equality in the mechanism's plenary sessions, dedicated thematic groups, dedicated intersessional meetings and review conferences and negotiations. As part of its functions, the mechanism can include:
    - Reporting on the gender balance of delegates participating in the mechanis
    - Sharing national gender- and equalities-disaggregated data and best practices on differentiated experiences of cyber incidents and cybersecurity measures as a regular procedural component of progress reports.
    - This may be facilitated and managed by the United Nations Office for Disarmament Affairs (UNODA)
- Considering the establishment of an additional ad-hoc dedicated thematic group with a focus on gender.

[16] Women's International League for Peace and Freedom (WILPF). (2022). *Advancing a Global Cyber Programme of Action: Options and priorities*. https://ict4peace.org/wp-content/uploads/2022/05/Report-Advancing-a-Global-Cyber-Programme-of-Action-Options-and-priorities.pdf

Annex 1 - Summary: Gender-responsive implementation of the UN Norms of Responsible State Behaviour in Cyberspace[17]

Norm	Gender-responsive implementation
a: Interstate cooperation	• Gender mainstream the voluntary checklist for practical action for norm implementation. • Align national cybersecurity strategies and WPS national action plans • Aim for gender parity and implement gender training for cyber diplomacy teams
b: All relevant information	• Collect gender-disaggregated data on effects of cyber incidents • Consult with civil society organisations to understand broader intersectional gender effects and consequences of cyber incidents
c: Prevention of ICT misuse	• Analyse conventional ICT misuse for gendered effects • Take measures to address ICT misuse against the rights of other states, affecting individuals and communities, including TFGBV
d: Cooperation to stop crime and terrorism	• Develop non-juridical measures to address TFGBV and other forms of cybercrime, including through cooperation schemes • Apply human rights safeguards in international cooperation to avoid adverse effects on basis of gender and/or sexuality
e: Human rights and privacy	• Recognise gender equality as a component of human rights in the digital age • Protect and promote encryption • Close the gender digital divide and digital skills gaps
f: No damage to critical infrastructure	• Consult with civil society organisations to generate a context-specific, gender-responsive definition of critical infrastructure • Share gender-responsive definitions of critical infrastructure and good practice for protection and resilience

[17] Millar, K., & Ferrari, V. (2025). Op. cit., p. 41.

g: Protection of critical infrastructure	• Conduct gender audits of past emergency response to cyber incidents • Gender mainstream critical incident planning, resourcing and response • Build capacity in both technical skills and gender analysis
h: Response to requests for assistance	• Analyse requests for assistance for human rights compliance and to avoid adverse effects on the basis of gender
i: Supply chain security	• Analyse emerging technologies for harmful hidden features and/or malicious dual uses with gender-differentiated effects • Include technology that facilitates gender-based violence in counter-proliferation regimes • Develop gender-responsive technical cybersecurity standards
j: Reporting of ICT vulnerabilities	• Conduct gender analysis of ICT vulnerabilities • Include civil society organisations in reporting and information sharing • Cultivate inclusive and respectful working environments
k: No harm to emergency response teams	• Aim for gender parity in computer emergency response teams and cyber incident emergency response teams • Involve diverse teams in decision making