APC POLICY EXPLAINERS

WHAT IS A GENDER-SENSITIVE APPROACH TO CYBER CAPACITY BUILDING?

DEFINITION

A gender-sensitive approach to cyber capacity building understands and considers the gendered impacts and implications of cyber threats, and calls for specific steps to address the needs, priorities and capacities of women and people of diverse sexualities, gender expressions and identities.

THE PROBLEM

Online gender dynamics reinforce or even amplify the social, economic, cultural and political structures – and inequalities – of the offline world, and malicious cyber operations can differently impact people based on their gender identity or expression. Thus, people in positions of marginalisation or vulnerability are at particular risk.

"Gender-neutral" projects do not consider these unequal gender power relations, or patterns of exclusion in the design or delivery of cyber capacity-building activities. Capacity building that is gender-unaware or "gender-neutral" perpetuates gender inequality, exclusion and discriminatory practices by failing to protect those at risk of marginalisation.

THE CHANGE WE WANT TO SEE

A gender-sensitive approach to cyber capacity building recognises and responds to the differential cyber and critical tech access, opportunities, resources, benefits and risks of women and LGBTQI+ 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.

Capacity building should respect human rights and should be gender-sensitive and inclusive, universal and non-discriminatory, and should promote principles such as participation, trans-parency, diversity and accountability. A gender-sensitive approach to cyber capacity building 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 meaningful inclusion of women and LGBTQI+ people in projects, activities, approaches and outcomes, and empowers them with various resources so that they can fully participate. 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.

In order to incorporate a gender-sensitive approach to cyber capacity building, states can draw upon relevant tools and frameworks such as the Women, Peace and Security Agenda, the Sustainable Development Agenda, and Human Rights Council reports and resolutions, among others. In addition, for instance, the final substantive report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security (OEWG) highlighted in 2021 that capacity building "should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory."

States should work together with non-governmental stakeholders to further develop a comprehensive definition of cybersecurity that incorporates a gender-sensitive approach. The role of civil society, in particular, is key in supporting states to adopt a rights-based and gender approach to ensure that there is trust and security in networks and devices that reinforce, rather than threaten, human security.

HOW APC WORKS ON THIS ISSUE

APC conducts research on a gender approach to cybersecurity (see our explainer on a gender approach to cybersecurity here) and a gender-sensitive approach to cyber capacity building, and monitors policy development on this topic at the global, regional and national levels. In addition, APC works collaboratively with its 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 human rights-based approach to cybersecurity, since humans are the ones impacted by cyber threats, incidents and operations (see here for our explainer on a human rights-based approach to cybersecurity).

At the global, regional and national levels, APC advocates for more open and participatory cyber policy processes. For instance, APC has consistently raised awareness on the need for a human rights-based and a gender-sensitive approach to cyber capacity building at international forums and groups such as the OEWG, from its inception in 2019.

Building on its research and advocacy work, APC also develops tools to support the work of different stakeholders in the cybersecurity space. For example, APC has published a framework to support policy makers and civil society organisations in achieving gender-responsive cybersecurity policies and strategies.

APC develops tailored trainings for women's rights activists so they can use the internet safely, such as the Feminist Tech Exchange (FTX), which seeks to be a feminist contribution to the global response to digital security capacity building.

APC also has been convening stakeholders and designing training that responds to local contexts. For example, the African School on Internet Governance (AfriSIG) is a capacity-building initiative whose goal is to strengthen the capacities of African leaders to participate in local and international internet discussions. The AfriSIG 2022 edition, for example, was focused precisely on international cybersecurity and capacity-building needs in Africa.

REGIONAL AND NATIONAL IMPLICATIONS

What happens in global cybersecurity discussions influences processes at the regional and national levels (and vice versa): global norms can have an important influence on what states do at the national and regional level. In order to be implemented, global norms on cybersecurity require policy and regulatory instruments, policies and frameworks. Increasingly, regional intergovernmental bodies are addressing cybersecurity, including the Organization of American States (OAS), the Association of Southeast Asian Nations (ASEAN), the African Union, and the European Union (EU). And worldwide, cyber-security is increasingly becoming a national policy priority.

WHERE IS THE DISCUSSION TAKING PLACE?

At the international level, cybersecurity has been debated at spaces such as the UN General Assembly First Committee and at the International Telecommunication Union (ITU).

In late 2018, the UN First Committee established two parallel processes to discuss responsible state behaviour in cyberspace: the UN Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG) (see here for an explainer on these processes). The ITU carries out a number of activities aimed at "Building confidence and security in the use of ICTs", including through the development of the Global Cybersecurity Agenda (GCA), as a framework for international cooperation in this area, and the Global Cybersecurity Index (GCI).

SOME SPACES AND INSTITUTIONS TO ENGAGE WITH

- International Telecommunication Union (ITU)
- Organisation for Economic Co-operation and Development (OECD) Committee on Digital Economy Policy, for instance, through the Civil Society Information Society Advisory Council (CSISAC)
- Global Forum on Cyber Expertise (GFCE)
- Organization of American States (OAS) Inter-American Committee against Terrorism (CICTE)
- UN Group of Governmental Experts (GGE) on advancing responsible State behaviour in cyberspace in the context of international security (GGE)
- UN General Assembly Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG)

READ MORE

A framework for developing gender-responsive cybersecurity policy (APC)

Why Gender Matters in International Cybersecurity (Women's International League for Peace and Freedom and APC)

APC statements at the OEWG

APC statement at the Intersessional Meeting of the Open-ended Working Group on ICTs: Engaging all stakeholders to enhance capacity-building efforts

Why should gender matter (more) for the OEWG? (Cyber Peace & Security Monitor)

OEWG Final Substantive Report

A rights-based approach to cybersecurity: A pipe dream or a critical means to a secure and stable internet? (APC)

Briefing document: Cybersecurity policy and human rights (APC)

Assessing National Cybersecurity Strategies from a Human Rights Perspective (Global Partners Digital)

Reaching Critical Will (Women's International League for Peace and Freedom)

Women's International League for Peace and Freedom inputs to the OEWG on capacity building

Gender Approaches to Cybersecurity (UNIDIR)

APC would like to thank Maia Levy Daniel, an external researcher, who supported the development of this explainer.

This publication was developed with support from the UK Government