APC POLICY EXPLAINERS

WHAT IS A GENDER APPROACH TO CYBERSECURITY?

- Definition
- The problem
- The change we want to see
- How APC works on this issue
- Regional and national implications
- Where is the discussion taking place?
- Some spaces and institutions to engage with
- Read more

DEFINITION

A gender approach to cybersecurity is a perspective that seeks to rethink individual and collective responsibilities for the cyber-security of individuals and groups, making cybersecurity responsive to the complex, differentiated and intersectional needs of people based on gender, sexual orientation, race, religion, ethnicity, ability, class and political affiliation, among other factors. It is not just about the rights of women, but centred on the human rights of people in the online context. That is why a gender approach to cybersecurity is closely linked to other agendas and principles, such as human rights and development.

A gender approach to cybersecurity encourages a re-evaluation of the concept of cybersecurity, which has traditionally been focused on the technical side of cybersecurity, often emphasising national defence or dealing with the needs of the financial industry. Instead, the focus is centred on the diversity of people and communities.

A gender approach to cybersecurity is about understanding and addressing the differentiated impacts, risks and needs faced by complex subjects (or individuals) in the context of cybersecurity. It questions and works to overcome the lack of intersectional diversity in a broad sense in cybersecurity. A gender approach to cybersecurity also promotes the creation and use of more nuanced gender and intersectional disaggregated data for more meaningful, impactful and informed policy decision making.

THE PROBLEM

People experience online threats differently based on their identities and experiences. Existing threats in cybersecurity – such as espionage, economic theft, intrusion or disruption of personal devices and networks, and internet shutdowns – have differentiated consequences depending on the gender of the individuals affected, among other intersectional factors.

However, since human rights are usually not considered when discussing international cybersecurity, less is known about how malicious international cyber operations between states affect people differently on the basis of gender or other characteristics that may put them in positions of vulnerability. Without a gender approach to cybersecurity policy and cyber norms discussions, decision makers make critical security decisions based only on assumptions and partial or incomplete information, leaving large segments of the population vulnerable to cyber threats and making it easier for cyber criminals and other malicious actors to exploit these information gaps and blind spots.

Technology and policies that deal with technology are not “neutral”. Rather, they contribute to – or can be made to mitigate – the hierarchies of social, economic and political power that create discrimination and inequalities. Cybersecurity policies should aim to mitigate intersectional inequalities and discrimination based on gender that are found in society, and this can only be done by acknowledging that these inequalities exist and developing remedies to address them. Thus, a gender approach strengthens human rights and improves national security.

A great challenge, however, lies in demonstrating how a gender perspective is not “just a women’s issue”. There is debate on the intersection of gender and cybersecurity and, while it is not yet easy to find consensus on the subject, it is even more challenging to find comprehensive examples of a gender approach to national cybersecurity policies. However, a few countries have attempted to offer a gender perspective on cybersecurity policy. These include, for instance:

Chile’s National Cybersecurity Policy (2017-2022)

According to this policy, the country would design and implement awareness campaigns, with an emphasis on vulnerable groups and implementing a gender perspective. In addition, as an objective, this cybersecurity policy emphasised that every measure proposed in the document needed to be designed and implemented from a human rights perspective and that, to achieve this goal, the country would implement a focus on gender, which would make visible inequalities that affect diverse groups in cyberspace and would enable ways to tackle them.

Eswatini’s National Cybersecurity Strategy (2022-2027)

The strategy builds on the 2022 National Development Strategy, aimed at addressing the critical dimensions of the quality of life including gender equity. Among its strategic goals, it includes fostering a safe and secure information society for Eswatini by, among other actions, developing tailored national awareness programmes and studies “targeting all groups of users, especially those who are vulnerable and at risk, such as children, women, senior citizens and other vulnerable groups.”

Icelandic National Cybersecurity Strategy (2022-2037)

In the introduction section, this document stresses the need to adopt cross-discipline values, and consider diversity and inclusion for those concerned (e.g. regarding education, gender, age and cultural background).

Cooperation is mentioned as an important factor and a prerequisite for achieving the strategy's objectives. Among the various aspects listed as "Main Emphases" in the Cooperation section, the document states that: "Emphasis is placed on diversity and inclusion, as cybersecurity is for all, and everyone should be enabled to participate. Particular attention shall be paid to increased participation of women in this respect."

THE CHANGE WE WANT TO SEE

A gender perspective in cybersecurity policy involves a systemic change. From the outset, in every step of the government's design, implementation and evaluation of cybersecurity measures, policies and norms, the goal must be to positively impact the greatest number of people in all their diversity and complexity of life situations. Gender needs to be understood as part of a complex and interlinked system of oppression. Accounting for these intersectional oppressions is fundamental to knowing and understanding the risks and needs faced by individuals in the context of cybersecurity.

Moreover, a gender approach also means recognising the importance of people who have agency in the process of creating a secure online environment. Unlike traditional views of cybersecurity that emphasise the passivity of subjects, a gender approach does not view people as mere passive recipients of cybersecurity measures.

In addition, states should involve all stakeholders for both the development and implementation of measures to address and respond to cyber threats. A gender approach entails ample participation of multiple stakeholders in cyber discussions, and empowering people for meaningful engagement in the design of cyber norms and policies.

States should work together with civil society and academia to further develop a comprehensive definition of cybersecurity that better understands the various existing and emerging threats that can affect people – for example, by rethinking threat-modelling practices and focusing on people's experiences with online threats. In particular, the role of civil society 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, 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 (our explainer on a human rights-based approach to cybersecurity can be seen here).

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 approach to cybersecurity at international forums and groups such as the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG), from the group's first substantive session 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. This framework consists of three main documents:

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

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, cybersecurity 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)
- Organization of American States (OAS) Inter-American Committee against Terrorism (CICTE)
- UN Group of Governmental Experts 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

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)

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