A FRAMEWORK FOR DEVELOPING GENDER-RESPONSIVE CYBERSECURITY POLICY: ASSESSMENT TOOL

APC
ASSOCIATION FOR
PROGRESSIVE
COMMUNICATIONS

A framework for developing gender-responsive cybersecurity policy: Assessment tool

This publication was developed and produced by APC with substantial support from external researcher Paz Peña.

Coordination and editing: Verónica Ferrari and Paula Martins (APC)

Editor: Alan Finlay

Proofreading: Lori Nordstrom (APC)

Design and layout: Cathy Chen (APC)

Published by APC 2023

APC would like to thank the following people and organisations for the feedback, time and expertise they contributed to support the development of this publication:

- Kerry-Ann Barrett, Katya Vera Morales, Orlando Garcés Corzo and all the team at the Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE), Organization of American States (OAS)
- Hija Kamran, Karla Velasco Ramos, Erika Smith, hvale vale and all the team at the APC Women's Rights Programme (WRP)
- Gabriela Montes de Oca, independent expert
- Nanjira Sambuli, Fellow, Technology and International Affairs, Carnegie Endowment for International Peace
- Daniela Schnidrig, Head of Engagement and Advocacy, National at Global Partners Digital
- James Shires, Isabella Wilkinson, Amrit Swali, Joyce Hakmeh and all the team at the International Security Programme at Chatham House
- Tatiana Tropina, Assistant Professor, ISGA, Leiden University
- Francisco J. Vera Hott, Programme Manager, Global Justice and Accountability, Open Society Foundations

ISBN 978-92-95113-60-2
APC-202306-GAPS-R-EN-DIGITAL-350

UK Government

This publication was developed with support from the UK Government.

Table of contents

I. INTRODUCTION TO THIS ASSESSMENT TOOL

This assessment tool seeks to provide step-by-step advice and concrete recommendations for those wishing to develop a gender approach to cybersecurity policy. Building on APC's previous work on a human rights approach to cyber-security, online gender-based violence, and cybersecurity and gender, ranging from research to advocacy, this document is part of a framework we have designed to support policy makers and civil society organisations in developing gender-responsive cybersecurity policies.[1]

This framework also includes two other documents, and we recommend that those using this assessment tool consult them before putting the principles and processes we outline here into practice:

- A literature review that explores how cybersecurity as a gendered space has been addressed in research.[2]
- 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.[3]

Drawing on the Cybersecurity Capacity Maturity Model for Nations (CMM),[4] this assessment tool offers a method of analysis based on the stage of maturity of

[1] In this assessment tool, national cybersecurity strategies and national cybersecurity policies are treated as synonymous. The principles of the framework can also be applied with some adaptation to cybersecurity laws and even regulations.

[2] APC. (2022a). *A framework for developing gender-responsive cybersecurity policy: Literature review*. https://www.apc.org/en/node/38416

[3] APC. (2022b). *A framework for developing gender-responsive cybersecurity policy: Norms, standards and guidelines.* https://www.apc.org/en/node/38411

[4] Global Cyber Security Capacity Centre. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM) - 2021 Edition.* https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

national policies in each country. Its focus is on the first three stages of maturity – what are called the "start-up", "formative" and "established" stages – given that these are the most important stages where policy can be influenced. It also adapts a tool for assessing national cybersecurity strategies from a human rights perspective developed by Global Partners Digital (GPD) as part of its analytical approach.

The recommendations made here are necessarily general and need to be adapted to be meaningful to particular contexts so that the transformative power of a gender approach to cybersecurity can be realised. While our focus is on the policy development process at the national level, the principles of the approach can also be applied in regional or global multilateral cybersecurity forums and discussions.

We hope this framework proves useful for policy makers and civil society actors, among others, who wish to build resilient, meaningful and relevant cybersecurity policy frameworks in their countries.

What do we mean by stages of maturity in this document?

The CMM defines stages of maturity for all dimensions and factors of cybersecurity capacity in a country. In this document, we focus on national cybersecurity policy, which, like all policy development, goes through an evolutionary process that is defined by contextual factors, including institutional and country resources, political will, and the skills and know-how of policy makers. While it is difficult to pinpoint exactly where policy processes are in terms of providing a comprehensive and meaningful response to cybersecurity needs for all, we talk generally of "stages of maturity".
The current stage of the policy development process in your country might actually be a mix of different stages.

Summary of key terms

Drawing on the literature review, the following are definitions used in this document:

Gender: The set of ideas, representations, practices and social prescriptions based on the anatomical difference between the sexes. These ideas and practices create social, economic and legal hierarchies in society that result in discrimination and inequality.

Gender mainstreaming: The process of assessing the implications for women and men of any planned action, including legislation, policies or programmes, in all areas and at all levels. Its ultimate goal is to achieve gender equality.

Intersectional perspective: The intersectional perspective identifies a system of diverse and interconnected oppressions – among them gender, but which include issues such as race, religion and class – that creates sometimes complex social, economic and other hierarchies among people in a society. Individuals are rarely subject to one form of oppression on its own.

Feminism: Feminism is a diverse and interdisciplinary approach to issues of equality and equity based on gender, gender expression, gender identity, sex and sexuality.

II. WHAT IS A GENDER APPROACH TO CYBERSECURITY?

A gender approach to cybersecurity policy is not just about the rights of women – it is a tool for developing policy that focuses broadly on the human rights of people in the online context. By this we mean that it is a perspective that seeks to make 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 a measure added to a policy that has already been designed; it is about a systemic change in the approach to cybersecurity. It encourages the creation and use of more nuanced gender and intersectional disaggregated data for more meaningful, impactful and informed policy decision making.

It encourages a re-evaluation of the concept of cybersecurity, which up until now has been focused on the technical side of cybersecurity, often emphasising national defence or dealing with the needs of the financial industry. Through our reframing of a country's approach to cybersecurity, the resilience of the national security system is strengthened.

What is a gender approach to cybersecurity?

A gender approach to cybersecurity is much more than just thinking about how cybersecurity impacts women. It is also about attending to intersecting discriminations and inequalities based on sexual orientation, race, ethnicity, ability, class and political orientation. It is a perspective that addresses the differentiated risks and impacts of cyber threats in order to make cybersecurity responsive to complex and differentiated needs, priorities and perceptions based on gender and other factors.

Common misconceptions

What to say when someone says:

- Gender is a "women's issue": No. Gender is about the social, political and economic hierarchies that have evolved that disempower or empower individuals based on their gender identity. It is also about how this identity intersects with other hierarchies or power and disempowerment based on issues such as race, religion and class.
- Cybersecurity is a technical issue only: No. 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 is "gender-blind": No. While cybersecurity policies should aim to mitigate intersectional inequalities and discrimination based on gender that are found in society, they can only do this by acknowledging that these inequalities exist and developing remedies to address them. Good cybersecurity policies are gender-aware rather than gender-blind.
- Feminism is just for women: No. Feminism is a social and political approach to systematically analysing and structurally bringing about change in society to make it more equal and respectful of human rights and dignity. Men can be feminists too.

III. WHY IS A GENDER APPROACH TO CYBERSECURITY IMPORTANT?

We believe that a gender approach to cybersecurity is a critical way to create policy that enables human rights online. 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. The challenge, however, lies in demonstrating how a gender perspective is not just a "women's issue". To do this we need to provide solid evidence that it is a transformative technical and policy approach to cybersecurity practices centred on the diversity of people and communities.

As can be seen in the literature review that accompanies this assessment tool,[5] there is debate on the intersection of gender and cybersecurity. While it is not yet easy to find consensus on the subject,[6] it is even more challenging to find comprehensive examples of a gender approach to national cybersecurity policies. In Latin America and the Caribbean, for example, Chile, Guatemala, Ecuador, Jamaica and the Dominican Republic were identified as countries that at some point[7] had national cybersecurity policies with "some general and explicit reference to a gender perspective or gender equity, but none established a roadmap and indicators to measure the progress and state of maturity of cybersecurity in light

[5] APC. (2022a). Op. cit.

[6] There are, however, signs of agreement in some areas, such as the need to close the digital gender divide, the need to address online and other technology-facilitated gender-based violence, and the need for more diversity in the cybersecurity sector and in general in technology. For example, see the Agreed Conclusions of the UN Commission on the Status of Women sixty-seventh session (CSW67): https://www.unwomen.org/en/csw/csw67-2023/session-outcomes

[7] For example, the current Dominican Republic strategy (2022-2030) does not include references to gender. However, the previous cybersecurity strategy (2018-2021) included references to gender equity. See more at: https://cncs.gob.do/wp-content/uploads/2020/02/Decreto-230-18.pdf

of this perspective."[8] An initial mapping by APC also identified some references to gender in the cybersecurity strategies of countries such as Eswatini, Iceland and Nigeria (as will be seen in greater detail later in this section).

Because of this, we believe it is essential to offer some sort of collective reflection on why it is important to include a gender approach in national cybersecurity policies. To this end – and as seen in the methodological note in section IV – we conducted interviews and held workshops[9] with specialists to better understand why a gender approach to cybersecurity policy is important, and how this approach differs from traditional cybersecurity policy-making processes.

The specialists offered powerful and compelling reasons why a gender approach to cybersecurity policy is important:

- **A gender approach benefits the greatest number of people:** A gender perspective in cybersecurity policy means that, from the outset, in every step of the government's design, implementation and evaluation of cybersecurity measures, the goal is to positively impact the greatest number of people in all their diversity and complexity of life situations. It is not a measure added to an already designed policy; it must take the form of a systemic change. This is because to have this positive impact, a gender approach to cybersecurity considers that cybersecurity threats affect people differently based on gender and different intersecting oppressions such as race and class, and this needs special consideration in cybersecurity deliberations. A consequence of this is that many of these oppressions that impact vulnerable groups are simultaneously addressed when a gender approach to cybersecurity is adopted. In this way, a gender approach to cybersecurity policy can be considered a way to help bring about systemic change in policy development.
- **A gender approach strengthens human rights and improves national security:** Without this systematic approach to cybersecurity policy, which includes gathering properly disaggregated data on gender and other intersectional challenges, large segments of the population are left vulnerable to cyber threats, making it easier for cyber criminals and other malicious actors to exploit these information gaps and blind spots. In other words, without a gender approach to policy, decision makers making critical security decisions will have made these decisions based only on assumptions and partial or incomplete information. As a consequence, national security as well as human rights are weakened.

[8] Herrera Carpintero, P., & Peña Ochoa, P. (2021). *Género y Ciberseguridad.* Centro de Estudios en Derecho Informático, Facultad de Derecho, Universidad de Chile.

[9] At the workshops, we used the definition of cybersecurity provided by the International Telecommunication Union (ITU): "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality." https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Our consultations also resulted in four interrelated insights that highlight how a gender approach to cybersecurity differs from traditional approaches to developing cybersecurity policy. Unlike traditional cybersecurity policy processes:

- **A gender approach is explicit that it is an intersectional approach:** Gender needs to be understood as part of a complex and interlinked system of oppressions. Accounting for these intersectional oppressions is fundamental to knowing and understanding the risks and needs faced by complex subjects (or individuals) in the context of cybersecurity. It also recognises that diverse security needs and practices that are meaningful to intersectional experiences must be acknowledged, including practices of care.[10]
- **A gender approach gives people agency:** A gender approach recognises the importance of active subjects who have agency in the process of creating a secure online environment. In other words, beyond recognising people from a gender and intersectional perspective and the oppressions these might imply, a gender approach does not think of people as passive recipients of cybersecurity measures. This understanding challenges the traditional view of cybersecurity that emphasises the passivity of subjects, including through the use of concepts such as "vulnerability".
- **A gender approach foregrounds equality and social justice in the policy-making process:** Using a feminist lens, a gender approach foregrounds human rights, as well as democratic principles such as participation, transparency and accountability.
- **A gender approach recognises the transformative potential of the policy-making process:** A gender approach recognises that cybersecurity policy-making processes can be transformative and challenge assumptions that may no longer work. For example, it questions the normative distinction between online and offline realities, seeks to rethink individual and collective responsibilities when it comes to the online security of individuals and groups, and broadens what is relevant to cybersecurity discussions. It also recognises that the design of technological solutions is not neutral, but often contributes to the "invisibility" of oppressed people.

[10] Practices of care, from a feminist perspective, are practised through social relationships, recognising the connections that exist between the personal and the structural – between our embodied experiences and the cultural norms, institutions and policies that govern support for care and caring; and care always involves relations of power. See Hoover, E. (2019, 29 October). Learning to care as a feminist. *openDemocracy*. https://www.opendemocracy.net/en/transformation/learning-care-feminist.
Acknowledging that the online and offline are indissociable, digital care is defined as a way to address digital security from a daily care perspective, and recognising that what affects our data also impacts our bodies. In the digital care perspective, taking care of our data is also taking care of our bodies, and this care should be done every day, as a habit, a culture, a politics. The digital care perspective aims to shelter the fear, not feed it. Methodologically, the work with digital care occurs with affection as the main conductor for learning, trusting it as a powerful way to structure exchanges and provide transformations. In addition, in digital care, work around safety is done from an integral perspective, understanding that the different spheres of the security field (such as physical, digital, psychosocial, etc.) are closely connected. See more at: https://fase.org.br/wp-content/uploads/2022/10/Digital-care-and-philanthropy.pdf

Some examples of a gender approach to cybersecurity policy[11]

Although they are hard to find, there are some examples of policies that have attempted to offer a gender perspective on cybersecurity policy. These include:

Chile's National Cybersecurity Policy (2017-2022)[12]

- This document highlighted that the country will design and implement awareness campaigns, with an emphasis on vulnerable groups and implementing a gender perspective. Also, 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 will implement a focus on gender, which will make visible inequalities that affect diverse groups in cyberspace and will enable ways to tackle them.

Ecuador's National Cybersecurity Strategy (2022-2025)[13]

- Under the strategy goal related to improving cybersecurity awareness, the strategy specifically establishes the development of programmes that will include "a perspective that takes gender equity into account."

Eswatini National Cybersecurity Strategy (2022-2027)[14]

- The strategy builds on the National Development Strategy from 2022, aimed at addressing critical dimensions of the quality of life including gender equity. Its strategic goals include fostering a safe and secure information society for Eswatini, by, among

[11] APC would like to thank Maia Levy Daniel, an external researcher, who worked on this mapping.

[12] The full strategy is available in Spanish at: https://www.cnc.cl/wp-content/uploads/2020/02/Pol%C3%ADtica-Nacional-Ciberseguridad.pdf; see more about the gender perspective in Chile's cybersecurity policy in this article, also in Spanish, by Paloma Herrera Carpintero: https://rchdt.uchile.cl/index.php/RCHDT/article/view/51577/61679 At the time of finalising this document, a new and updated cybersecurity policy was being discussed in Chile. The national policy was expected to be published at the end of May 2023, after a public consultation. In an interview on the issue, Cybersecurity National Coordinator Daniel Álvarez stressed that gender was one of the cross-cutting themes of the new strategy. See more at: https://www.df.cl/df-lab/transformacion-digital/coordinador-nacional-adelanta-los-principales-ejes-de-la-nueva-politica

[13] https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf

[14] https://www.esccom.org.sz/about/strategy/Eswatini%20National%20Cybersecurity%20Strategy%202022-2027.pdf

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."

Nigeria's National Cybersecurity Policy and Strategy (2021)[15]

- In the chapter on strengthening the legal and regulatory framework, the strategy includes a section on "gender rights online" that recognises the rights and importance of the active involvement of women in the use of cyberspace. The strategy expresses a commitment to "promote the inclusiveness and active participation of women in the complete lifecycle of activities in our cyber ecosystem" and commits to addressing "the barriers hindering accessibility for women." In the document, combating online violence against women also appears as a priority for the Nigerian government. Also mentioned is the promotion of online safety awareness and education for women and "the development of a multi-stakeholder forum to drive the development of online gender protection and participation initiatives," together with a commitment to provide the necessary support for organisations anchoring gender promotion initiatives to strengthen advocacy and to develop mechanisms to empower women and create opportunities in the cybersecurity ecosystem.

Icelandic National Cybersecurity Strategy (2022-2037)[16]

- In its introduction, 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.
- The strategy puts emphasis on cooperation, diversity and inclusion, "as cybersecurity is for all, and everyone should be enabled to participate," and it states that "particular attention shall be paid to increased participation of women in this respect."

[15] https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf?ref=benjamindada.com

[16] https://www.stjornarradid.is/library/04-Raduneytin/Haskola---idnadar--og-nyskopunarraduneytid/Icelandic%20National%20Cybersecurity%20Strategy%202022-2037.pdf

Jamaican National Cyber Security Strategy (2015)[17]

- The strategy includes as an objective that “measures are implemented to protect vulnerable groups in cyberspace.” The activities related to this objective for the medium to long term include implementing programmes that promote the adoption of safe practices online by vulnerable groups, including children, women and elderly people, among others.

Spain’s National Cybersecurity Strategy (2019)[18]

In the section on cybersecurity in the international sphere, when detailing the objectives regarding collaboration, the Spanish strategy mentions that the country will “collaborate in capacity building in third-party states, paying particular attention to women and young people, and will promote the creation of channels for the exchange of information and experiences, encouraging the adoption of bilateral and multilateral agreements in this field for these purposes.”

Singapore Cybersecurity Strategy (2021)[19]

- The document states that the government will work with all stakeholders to support youth, women and mid-career professionals to pursue a cybersecurity career.
- As a way to “grow a robust cyber talent pipeline,” the strategy highlights the need to “attract diverse talent”: “Apart from youths, the Government is also looking to attract more women and mid-career professionals from adjacent fields to join the cybersecurity industry.” The government will also “work closely with industry and international partners to encourage girls to take up cybersecurity education programmes and inspire women to take on cybersecurity roles.”
- The Cyber Security Agency of Singapore, under this strategy, launched SG Cyber Women, a targeted initiative to encourage more women to pursue a career in cybersecurity.

[17] https://www.mset.gov.jm/wp-content/uploads/2019/09/Jamaica-National-Cyber-Security-Strategy-2015.pdf
[18] https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019
[19] https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021

IV. A NOTE ON METHODOLOGY

This assessment tool has been developed through desk research together with in-depth interviews with gender and cybersecurity specialists from different regions and backgrounds. As stated before, this document draws from and was informed by the literature review and the norms document. As part of the methodology, we also organised a session during RightsCon 2022 that served as a first opportunity to collect impressions and feedback on this tool and to brainstorm with a diverse group of participants on how to incorporate a gender approach in cybersecurity policy. In July 2022, a validation workshop, with activists, civil society representatives, policy makers, international delegates and academics working on gender, cybersecurity and technology from different geographies, where key elements of this document were presented for feedback, was also organised.

During 2023, gender and cybersecurity specialists working in different sectors were also invited to review the text and provide additional input and to suggest changes. Lastly, in May 2023, we organised a feedback workshop with policy makers working at national and regional levels in Africa, where a summary of the key recommendations in this text were reviewed.[20]

In the absence of any particular framework for analysing gender in cybersecurity policies, one of the most difficult challenges is finding a common language that can make sense to a wide range of stakeholders from different regions.

With this in mind, we decided to use the Cybersecurity Capacity Maturity Model for Nations (CMM) created by the Global Cyber Security Capacity Centre of the University of Oxford.[21] The CMM is a framework developed to review the cybersecurity capacity maturity of a country across five dimensions and at different stages of maturity (see below). Although this model does not consider gender and

[20] APC would like to thank the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) and Media Foundation for West Africa (MFWA) for their collaboration in the organisation of this workshop.

[21] Global Cyber Security Capacity Centre. (2021). Op. cit.

it is a framework open to critical scrutiny, its wide adoption across regions makes it a worthwhile model to work with. It has been adopted and implemented in over 80 countries worldwide thanks to the collaboration of international organisations such as the Organization of American States (OAS), the World Bank, the International Telecommunication Union (ITU), the Commonwealth Telecommunications Union and the Global Forum on Cyber Expertise. It also offers a common language that can be strategic in framing conversations around gender, as well as a staged model that can help to guide the inclusion of a gender approach in cybersecurity policy depending on the national context. One of the conclusions reached following the in-depth interviews was that the gender approach in cybersecurity is a long-range work, as it depends on each country's cultural and political conditions for it to be incorporated to a greater or lesser extent. This implies that there are evident differences between countries when evaluating the incorporation of gender in national cybersecurity strategies: some will have more mature levels than others. Considering these arguments, the CMM is a good tool in its adaptability to the different realities that the people using this tool face.

As one of our analytical tools we also adapted the document "Assessing National Cybersecurity Strategies from a Human Rights Perspective",[22] developed in 2022 by Global Partners Digital (GPD). The document identifies six essential components that are necessary for developing a national cybersecurity policy and gives general recommendations as to what should be included in those components from a human rights perspective. Human rights and the gender approach to cybersecurity are related: both look at people as the centre of any cybersecurity strategy. In this sense, the framework put forward by GPD offers a conducive space to build on and adapt it to the gender approach.

As mentioned earlier, this assessment tool is accompanied by two other resources that were developed prior to drafting this document.[23] They provide a reference point for our discussions here and informed much of our contextual thinking on the subject of gender and cybersecurity. These documents are:

Literature review

The literature review explores how cybersecurity as a gendered space has been addressed in research, as a contribution to promote more gender-sensitive cybersecurity policy. In this review, you will find:

- Important concepts on gender.
- General background context on the development of the concept of cybersecurity as a gendered space.

[22] Global Partners Digital. (2022). *Assessing National Cybersecurity Strategies from a Human Rights Perspective.* https://www.gp-digital.org/wp-content/uploads/2022/04/Assessing-NCSS-from-human-rights-perspective.pdf

[23] Both can be found here: https://www.apc.org/en/pubs/framework-gender-cybersec

- Connections between the emergence of human rights in cybersecurity and a gender perspective and the most prevalent cross-cutting concepts that appear in the different research that takes gender into account in the various fields of cybersecurity.
- Discussion on some of the topics where the gender perspective in cybersecurity is more present.

Norms, standards and guidelines

There are relevant tools, agendas and frameworks that cybersecurity advocates can draw upon when seeking to promote a gender perspective within national or multilateral cybersecurity discussions. These can be used as a source of information or to establish policy coherence with a government's existing commitments to gender equality. This document presents an overview of the most relevant of these instruments:

- The Convention on the Elimination of all Forms of Discrimination against Women (CEDAW)
- The Beijing Declaration and Platform for Action
- The Women, Peace and Security (WPS) Agenda
- The outcome documents of the World Summit on the Information Society (WSIS)
- The 2030 Agenda for Sustainable Development and the Sustainable Development Goals (SDGs)
- UN Human Rights Council (HRC) reports and resolutions
- International Telecommunication Union (ITU) initiatives
- UN General Assembly cybersecurity processes.

V. WHO IS THIS ASSESSMENT TOOL INTENDED FOR?

We intend our framework – this assessment tool, the literature review, and the summary of norms, standards and guidelines – to be useful for different audiences and in different ways. It is mainly intended for policy makers working on cybersecurity strategies and policies and as an advocacy tool for civil society organisations working on cybersecurity and advocating at the national level. A secondary audience is regional organisations influencing policies on cybersecurity at the national level, and international organisations developing guidance on how to draft national cybersecurity strategies. It also aims to be useful to both these audiences when they engage in global spaces related to cybersecurity and multilateral discussions. Finally, we hope it is useful more widely for civil society organisations and researchers involved in gender and cybersecurity.

VI. HOW WE USE THE CYBERSECURITY CAPACITY MATURITY MODEL FOR NATIONS (CMM)

The CMM sees the development of cybersecurity policy as consisting of five distinct stages of maturity: start-up, formative, established, strategic and dynamic. It also articulates five dimensions that constitute the broad range of capabilities that a government needs to deliver cybersecurity effectively. These are:

1. Developing cybersecurity policy and strategy.
2. Encouraging responsible cybersecurity culture within society.
3. Building cybersecurity knowledge and capabilities.
4. Creating effective legal and regulatory frameworks.
5. Controlling risks through standards and technologies.

Lastly, each dimension has four aspects that need consideration: strategy development, content, implementation and review,[24] and international engagement.

[24] In contrast to the CMM, the content aspect has been merged with the implementation and review aspect in this assessment tool. The reason is practical: it is necessary to have the content of the national cybersecurity strategy in order to ensure a mechanism for monitoring, coordination and review of the policy. In this sense, this tool grouped them together as a single aspect since it works transversally with recommendations for gender mainstreaming and, especially, in the policy's formative stage with recommendations for coordination, monitoring and review mechanisms.

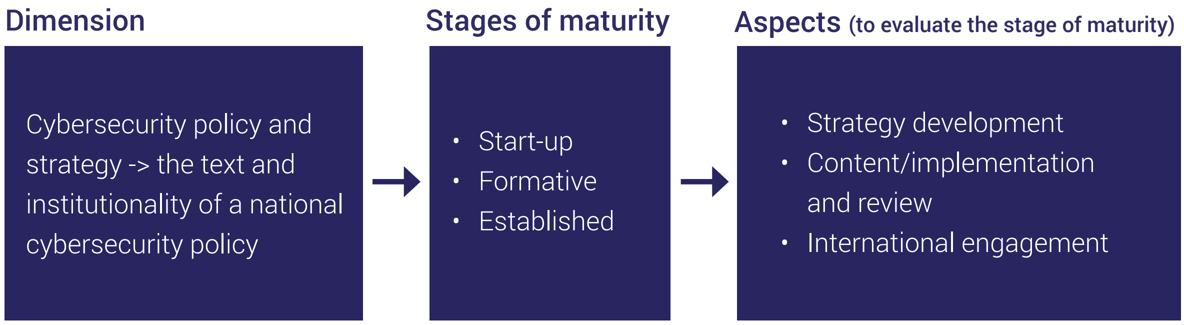
This assessment tool adapts this model to help policy makers and civil society organisations assess how they can introduce a gender perspective into their national cybersecurity policy processes. Our focus is on:

- National cybersecurity strategy, which is a factor of the CMM dimension "Developing cybersecurity policy and strategy".
- The first three stages of maturity: start-up, formative and established.

In the remaining two stages of the CMM ("strategic" and "dynamic"), a national cybersecurity policy has been published and an institutional framework is in place. In this document, these final two stages are referred to as a "vision" to be achieved with a national cybersecurity policy that considers the gender approach to be a fundamental part of its deployment.

As the CMM states:

> National cybersecurity strategy [Factor D.1.1 under dimension 1] is essential to mainstreaming a cybersecurity agenda across government because it helps prioritise cybersecurity as an important policy area, determines responsibilities and mandates of key cybersecurity government and non-governmental actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities.[25]



Dimension

Cybersecurity policy and strategy -> the text and institutionality of a national cybersecurity policy

Stages of maturity

- Start-up
- Formative
- Established

Aspects **(to evaluate the stage of maturity)**

- Strategy development
- Content/implementation and review
- International engagement

Table 1 summarises the first three stages of maturity, highlighting the key objectives to be targeted in each stage. Instead of the word "strategy", which is used in the CMM, we refer to "policy". The rest of this document discusses recommendations for actions aimed at meeting the goals for each of these stages.

[25] Global Cyber Security Capacity Centre. (2021). Op. cit.

GENDER IN NATIONAL CYBERSECURITY POLICY

Start-up stage

To raise awareness among stakeholders of the importance of the gender approach to cybersecurity.

Strategy development

To understand national cybersecurity risks and threats from a gender perspective.

Content / implementation and review

To analyse legal frameworks and policies that can respond to the gender needs and challenges raised above, even if only partially.

International engagement

To map the government's knowledge and engagement with international debates on gender and cybersecurity or related subjects, such as internet governance and gender, gender and STEM, gender perspectives of cybercrime.

Formative stage

To include the gender approach in the various strategic aspects of the cybersecurity policy and its action plan.

Strategy development

To conduct a national risk assessment to collect information and evidence on the intersectional risks faced by people in the context of cybersecurity, identifying gaps in current security mechanisms.

To enable inclusive consultation mechanisms.

Content / implementation and review

To influence the different components of the development of the national cybersecurity policy, including by providing content on gender.

To ensure that actions with a gender focus are prioritised in the action plan.

International engagement

To engage together with authorities in regional and global forums and processes in order to initiate or deepen an understanding of cybersecurity and gender in the international context.

Established stage

To actively participate in evaluating the results of the policy and to participate in national and international cooperation to strengthen the gender approach to cybersecurity.

Strategy development

To evaluate whether the policy's implementation actions comply with the proposed goals and present evidence to support any necessary follow-up mechanisms.

Content / implementation and review

To create instances of dialogue, knowledge sharing and mutual cooperation with other public policies that could be related to gender or cybersecurity.

International engagement

To facilitate instances of knowledge about the government's participation in regional and international forums, consult inputs, and seek to coordinate the positioning of the gender issue in cybersecurity.

VISION

After these three stages:

The gender perspective is considered strategic in cybersecurity by all stakeholders.

The gender perspective in cybersecurity has a tangible positive impact on the robustness and resilience of infrastructure in the face of attacks, has strengthened human rights for the diversity of people in cyberspace, and has had a positive impact on mainstream and dynamic cybersecurity cultures at the corporate and societal levels.

The country has become a champion of the gender perspective in cybersecurity at the regional and international levels.

What do we mean by stages of maturity?
While it is difficult to pinpoint exactly where policy processes are in terms of providing a comprehensive and meaningful response to cybersecurity needs for all, we talk generally of "stages of maturity". The current stage of the policy development process in your country might actually be a mix of different stages.

A. START-UP STAGE

At this stage, the discussion on cybersecurity and gender is new to most stakeholders. Therefore, the objective of this stage is to create awareness among the various stakeholders of the importance of the gender approach to cybersecurity.

a. Strategy development aspect

Although a national cybersecurity policy does not yet exist at this stage, planning processes for strategy development may be underway. The focus on strategy development should be primarily twofold: first, understanding the national cybersecurity risks and threats from a gender perspective through research and an inclusive consultation process; and second, having understood and acknowledged the risks and threats, raising awareness of the importance of a gender approach to cybersecurity and the risks and threats you have identified among policy-making stakeholders.

These consultation processes are a way to build evidence that will impact on the specific policy decisions you make and what needs to be prioritised and included. In order to build this evidence, you can follow the different actions described below. These do not follow any particular order and their usefulness should be evaluated according to the contextual possibilities of each country.

RECOMMENDATIONS

Identify a gender and cybersecurity champion within the government:

The champion does not need to be someone who is a gender expert, but rather someone who firmly believes in how vital it is to incorporate this perspective into a national cybersecurity policy so that it responds to the country's challenges. The champion also does not have to work in cybersecurity. Their presence unlocks processes and drives initiatives.

Frame a gender approach to cybersecurity broadly:

Emphasise that although issues such as the participation of women and online gender-based violence are critical, a gender approach to cybersecurity is much broader than this and also covers issues such as understanding the differentiated risks and impacts of cyber threats on the basis of gender and other intersectionalities; the different cybersecurity needs, priorities and perceptions based on gender and other factors; and what cybersecurity capacity building should look like from a gender intersectional perspective. A gender approach to cybersecurity is about approaching cybersecurity with an understanding of the intersectional impacts of cybersecurity policy. This means that a gender approach to cybersecurity may be relevant to a number of other departments or ministries in government.

Key questions to ask in this strategic development phase include:

- What are the risks and consequences of specific threats in cyberspace for people such as public figures, human rights defenders and journalists, and people in situations of marginalisation or vulnerability due to their gender, race, religion, ethnicity, ability, class, political affiliation or sexual orientation?
- What are the capabilities, needs and priorities of different genders and their intersectionalities when it comes to cybersecurity?
- How do gender norms shape priorities within cybersecurity designs in your country?
- What are the gender and cybersecurity knowledge gaps in your country today?
- Who are the relevant actors from different sectors committed to adopting a gender perspective in cybersecurity?

A general mapping of a wide range of stakeholders

It is critical to find the voices that can help understand how gender impacts on cybersecurity in each country. As seen in the literature review accompanying this assessment tool, there are many nodes in cybersecurity where gender has been studied.[26] It is recommended that you use these nodes as a starting point to identify actors and stakeholders who are already working on issues to do with gender and cybersecurity or in a field that is relevant to the topic (see Table 2).

.

[26] Review the section "Critical nodes of cybersecurity for a gender perspective" in the literature review that forms part of this framework: APC. (2022a). Op. cit.

Table 2: What actors have worked locally on gender-related issues in cybersecurity?

Actors	Critical nodes of cybersecurity from a gender perspective
Civil society Technical sector Private sector Academia State agencies and departments	• The gender gap in the cybersecurity field (industry and policy) • The dimensions of gender-based violence in cybersecurity • Differential vulnerabilities to cyber attacks (internet access and digital skills; demographic factors in cybersecurity behaviour) • Differential impact of cyber incidents based on gender • Reconfiguring cybersecurity analysis frameworks • Feminist autonomous internet infrastructure[27] • International public policies on cybersecurity

It should be remembered that at this stage there are rarely many actors working directly on gender and cybersecurity issues, so it is strategic to broaden the consultations to actors who may eventually be interested in cybersecurity, such as organisations working on women's rights or sexual rights, or on youth, race or ethnicity, among other intersectional areas. This mapping will allow you to identify potential strategic partners that will be able to participate in the various actions needed to introduce a gender perspective into cybersecurity policy, including awareness raising and capacity building.

Awareness of gender and cybersecurity among various identified stakeholders

Raising awareness of the critical relationship between gender and cybersecurity is key at this stage, as it may later be part of formal capacity-building planning in the formative stage of the national cybersecurity strategy. Stakeholders can be grouped into two broad categories – those who know about gender and intersectional issues, and those who know about cybersecurity – and the focus of your awareness-raising processes will be different for each.

[27] For more information on feminist infrastructures, see: Toupin, S., & Hache, A. (2015). Feminist autonomous infrastructures. In A. Finlay (Ed.), *Global Information Society Watch 2015: Sexual rights and the internet*. APC & Hivos. https://www.giswatch.org/index.php/en/internet-rights/feminist-autonomous-infrastructures; Zanolli, B., Jancz, C., Gonzales, C., Araujo, D., & Prado, D. (2018.) Feminist infrastructure and community networks: An opportunity to rethink our connections from the bottom up, seeking diversity and autonomy. In A. Finlay (Ed.), *Global Information Society Watch 2018*: *Community networks*. APC & IDRC. https://www.giswatch.org/en/infrastructure/feminist-infrastructures-and-community-networks

Raising awareness about the importance of cybersecurity among actors working on gender or women's rights issues, as well as related intersectional issues

It is uncommon for stakeholders working on these issues to necessarily know about cybersecurity or think of national cybersecurity policy as an important space for advocacy. Working with these actors to create an awareness of the importance of cybersecurity has multiple benefits: it increases their interest in cybersecurity, which can translate into projects such as capacity-building initiatives or research to generate evidence for policy; it strengthens relationships between actors; and it builds the technical language and knowledge of cybersecurity among actors so that they can participate not only in the design of the policy but also in its implementation. One of the most important outcomes of this process is that it will help you identify and map contextual and intersectional risks and challenges faced by people from a gender perspective, which will feed into your policy process.

Raising awareness of the importance of a gender approach among cybersecurity actors

The accompanying literature review to this assessment tool identifies various aspects of cybersecurity where a gender approach is important. It is recommended that the issue of a gender approach is introduced focusing on these aspects.

Both of these processes will be important when you move to the formative stage, where the benefits of having informed actors engage in discussions on a gender approach to cybersecurity will be felt.

International consulting

You may need to ask different international partners such as policy makers from other countries, academics, experts from institutions or civil society specialists for advice on the cybersecurity strategy at this start-up stage. It is important to map the various gender and cybersecurity specialists who can support a country in this area. For instance, there may be governments that have taken as their mission the mainstreaming of gender in public policies, and who can advise on good practices in this area. As seen in the literature review, there are also many professionals and organisations working on the Women, Peace and Security Agenda who have deepened their relationship with cybersecurity, and who can offer direction and advice. The private sector should also be considered, as many companies have made strides in incorporating diversity in the workforce in the cybersecurity industry. While these actors can inform the policy-making process, they are also potential allies in future negotiations in global forums.

International institutions can help your policy-making process

More and more institutions are building evidence on the importance of a gender approach to cybersecurity. Here are just a few organisations you could consult:

- Association for Progressive Communications (APC) – https://www.apc.org
- Global Partners Digital (GPD) – https://www.gp-digital.org
- Chatham House – https://www.chathamhouse.org[28]
- United Nations Institute for Disarmament Research (UNIDIR) – https://unidir.org[29]
- Women's International League for Peace and Freedom (WILPF) – https://www.wilpf.org/
- Geneva Centre for Security Sector Governance (DCAF) – https://www.dcaf.ch

b. Content/implementation and review aspects

In the start-up stage, the "content" aspect involves collecting local evidence, reviewing available local and global research on the issue of gender and cybersecurity, and reviewing national and global policy documents that are relevant to your work.

RECOMMENDATION

Collect case studies, reports and policy examples:

Look for reports that are relevant to your national context and that reflect global research and policy development processes. Make sure you gather reports that account for the wide range of gender and other intersectionalities (e.g. sexual orientation, race, class). Review gender policies in other areas that may impact on your work, such as affirmative action policies in STEM careers, or policies on online gender-based violence. It is useful to make a note of specific policy wording or phrasing that you think will be useful.

[28] https://www.chathamhouse.org/about-us/our-departments/international-security-programme/understanding-gender-and-cybersecurity

[29] https://unidir.org/programmes/gender-and-disarmament

Gathering evidence

The start-up phase's central goal is to gather evidence on the state of cybersecurity in the local context. For this reason, collecting a wide range of studies and reports that account for how gender and other intersectionalities are relevant to cybersecurity is critical, as are the awareness-raising processes discussed above, where contextual risks and challenges can be identified. The mapping of actors is also useful as it also allows us to identify any work they have done in gathering quantitative and qualitative evidence relevant to our policy-making process.

However, when there is little local evidence that has been published – which is common because it is a topic still in its infancy – you may want to create focused case studies as a way of documenting the intersectional impact of cybersecurity mechanisms in the local context. The resources you have will determine the breadth of this research. For example, you may want to develop case studies in a particular field only, such as the impact of the absence of a gender perspective in Computer Security Incident Response Teams (CSIRTs),[30] the gendered impact of specific incidents such as ransomware or data breaches, or the impact of affirmative action policies in STEM careers. However, when presenting your case studies, you should frame them as examples within the broader integrated gender approach to cybersecurity policy.

While the aim of this stage is to collect local evidence to support your policy-making process, regional and international studies can be used to better understand the challenges that countries face across the world in this area.

Another important part of the "content" aspect is reviewing national policies and strategies related to cybersecurity (for example, national digital strategies, or national strategies on artificial intelligence). You need to understand whether and to what extent they reflect gender-specific priorities. Policies from intersectional fields that are relevant to a gender approach to cybersecurity also need to be reviewed, such as gender strategies, inclusion and diversity policies or STEM policies. Relevant legal frameworks such as those dealing with online gender-based violence or laws on data protection should also be reviewed.

[30] Teams of technical and other experts set up to respond to security breaches or incidents.

c. International engagement aspect

RECOMMENDATION

Map how the government engages on relevant issues:

Map the government's knowledge and engagement with international debates on gender and cybersecurity or related intersectional topics. This mapping should include a good understanding of the government's engagement in cybersecurity and internet governance forums or spaces where the issue of women and information and communications technologies (ICTs) are dealt with.

This aspect explores the extent to which the government and other relevant stakeholders such as civil society or business engage in international debates and forums on cybersecurity policy.[31]

While you can expect to find some engagement in cybersecurity forums, you are likely to find that at least when it comes to the government, this engagement does not promote a gender perspective on cybersecurity. However, it is important to map how this engagement occurs, and which forums are engaged. The engagement of stakeholders in related forums such as those on internet governance or discussions on gender and ICTs is also important. By mapping this engagement, you will better understand the gaps in the knowledge of key stakeholders in the policy-making process, and where this knowledge needs to be strengthened.

[31] For more background, see the accompanying publication on relevant existing international norms, standards and guidelines connected with gender and cybersecurity: APC. (2022b). Op. cit.

B. FORMATIVE STAGE

At this stage, through background research, awareness-raising processes and gathering local evidence of risks and challenges, the key priorities of a gender approach to cybersecurity policy in your local context should have been mapped. This stage involves drawing on this evidence to ensure that your findings influence and shape the drafting of the cybersecurity policy and action plan.

a. Strategy development aspect

The CMM recognises that at the formative stage, the policy development process has already begun and that a first outline of the national cybersecurity policy has already been articulated. In addition, further consultation processes with key stakeholder groups have already been agreed upon, where the actual text of the emerging policy document will be discussed. Two aspects of strategy development should be carefully considered:

National risk assessment

Before developing content for your policy, it is important to develop a national risk assessment. This can provide valuable information for developing, executing and evaluating a policy. Governments commonly use national risk assessments in policy-making processes.

It is important that this assessment identifies the specific risks that individuals might face due to their gender or related intersectional oppressions. Much of the evidence for this national risk assessment would have already been gathered in the start-up stage. However, you may have identified gaps for further engagement. You might also need to conduct a much broader assessment that maps all the risks faced by other sectors and actors that you did not engage in your start-up phase.

The national risk assessment creates a comprehensive picture of interlinked risks that will ensure that your policy responds properly to those that have been identified. At this point you may want to articulate the draft outline of your policy building on what you have developed and to see if there are gaps that you can already identify.

Consultation mechanisms

The participation mechanisms for consulting on the policy drafts are important. They are a way of strengthening trust and collaboration between stakeholders impacted by the cybersecurity policy. They should be inclusive, and facilitate sector, specialist and broad-based input.

Different mechanisms such as meetings and online processes for input into the policy drafts should be set up. These should be appropriate to the capacity and resources of the stakeholders. These mechanisms should also allow stakeholders adequate time to review the drafts and provide input.

Spend some time deciding what participation mechanisms are important. These processes are important because the expectations of different stakeholders must be managed from the outset. The mechanisms and limits of participation must be transparent to stakeholders, and, to avoid an imbalance in the voices from different sectors or groups, consultation processes and spaces must be designed to be broadly representative, including in how they are convened, where they are convened, and how the conversations are facilitated.

You should contemplate accountability mechanisms to make sure inputs are incorporated and stakeholders are being updated on the status of the process and how their inputs are being incorporated. If the participation processes are inclusive and carefully thought out, they will allow stakeholders to commit to the policy and the success of its implementation.

Regarding the call for participation in consultations, you should make sure to include the stakeholders you have engaged in the start-up stage. This ensures continuity, and that those most affected by cybersecurity threats are represented.

RECOMMENDATIONS

Design the participation processes carefully to ensure inclusion:

Building a gender approach to cybersecurity is not just about policy makers sitting around a table, but about broad-based consultation on the issue. Think about who needs to be involved in discussions from a gender and intersectional perspective. This may include individuals from across government departments, NGOs working with marginalised groups, or business associations. Key government departments you may want to include in the process are those dealing with women and LGBTQIA+ people's rights, child protection, digital inclusion, promoting equality and diversity, and combating disinformation.

Pay attention to power dynamics:

Think about the processes of engagement, paying particular attention to power dynamics and how to make sure the most vulnerable groups have a voice. If you are meeting face to face, ask practical questions such as, "How far do participants have to travel to get there?" If you are meeting online, understand the cost commitments that some participants might have to make to participate, such as paying for data.

Civil society participation

From a civil society perspective, these consultation mechanisms are an opportunity to present the risks and threats to national cybersecurity from a gender perspective and to advocate for specific policy priorities in this regard. The consultation mechanisms will also provide an opportunity to evaluate the likely outcomes of the policy and its implementation.

Civil society should consider using the consultation mechanisms as an opportunity to coordinate with other organisations so that a common front is presented. Actors will need to map available evidence that supports a gender and intersectional approach to cybersecurity policy so that they can clearly communicate the risks and challenges faced by intersectional communities. The relationship between gender and cybersecurity must be presented as more than a "women's issue" to avoid any resistance that may be encountered in the discussions, and to show how a gender approach has cross-sectoral relevance. In this sense, the most common nodes of cybersecurity and gender presented in the literature review document can be a basis for guiding the intervention of civil society.[32] Finally, civil society should strategically adapt its evidence and positions to the technical language used in cybersecurity discussions so that it is more natural for decision makers to see the relationship between cybersecurity and gender.

[32] The critical nodes of cybersecurity from a gender perspective are: the gender gap in the cybersecurity field (industry and policy); the dimensions of gender-based violence in cybersecurity; differential vulnerabilities to cyber attacks (internet access and digital skills; demographic factors in cybersecurity behaviour); differential impact of cyber incidents based on gender; reconfiguring cybersecurity analysis frameworks; feminist autonomous internet infrastructure; and international public policies on cybersecurity.

b. Content/implementation and review aspects

RECOMMENDATIONS

Provide a broad framework of policy arguments:

Many specialists agree that public policy decision makers need arguments beyond those specific to cybersecurity and gender to be able to unite political wills. Among the suggestions, they highlight linking with:

- Regional and international commitments. For example, how cybersecurity and gender relates to the Sustainable Development Goals (SDGs) or the Women, Peace and Security (WPS) Agenda set forth by the United Nations.[33]
- Digital economy. Build arguments and show indicators of how this perspective allows the strengthening of the digital economy – for example, in relation to facilitating employment and labour market participation of women, and diversity in entrepreneurship.[34]
- International cooperation. Many countries and international cybersecurity forums may be particularly interested in gender mainstreaming in cybersecurity; their expertise and support can be substantive for local decision makers.

Include the perspectives of all the stakeholders you have engaged:

- Ensure that the needs and perspectives of the broad range of stakeholders you have engaged during the strategic development process are taken into consideration. Make these available in succinct summaries for policy makers so that they can be easily referred to.

[33] Please see more about these connections in APC. (2022a). Op. cit.

[34] See, for example: Organisation for Economic Co-operation and Development. (2018). *Bridging the Digital Gender Divide: Include, upskill, innovate*. https://www.oecd.org/digital/bridging-the-digital-gender-divide.pdf

At this formative stage, there is a draft with the content of the policy which should reflect the country's specific cybersecurity priorities and circumstances, including those raised from a gender perspective.

It is important at this stage to remember that the gender perspective is intrinsically part of the human rights framework that most governments have committed to. We refer to this as a rights-based approach to policy development.[35] For example, UN Women has stated that it is crucial to link gender mainstreaming and human rights-based approaches in development policies and programmes, since gender equality, non-discrimination based on sex and gender identity, and access to sexual and reproductive health and rights are fundamental universal principles of human rights.[36] Making this link clear to policy makers is important because it emphasises that the government already has pre-existing commitments to implementing a gender approach to cybersecurity policy. It is also important to take note of the links between the cybersecurity policy and other policies, such as national ICT policies or broadband policies, to see if changes need to be made to those policies so that a gender approach to cybersecurity policy is coherent across national policy spaces.

The document "Assessing National Cybersecurity Strategies from a Human Rights Perspective",[37] elaborated by Global Partners Digital (GPD), offers a solid base on which a gender perspective can build. The GPD document identifies six core components that are systematically included in the recommendations for developing a national cybersecurity policy and, in turn, gives general recommendations as to what basic elements should be included in those components from a human rights perspective. These recommendations are adapted in Table 3 to offer guidance to policy makers and civil society organisations on how they can introduce a gender perspective into their national cybersecurity strategies.

Regarding implementation and review, a coordinated action plan for implementing the cybersecurity policy is just being developed at the formative stage. Generally, implementation design occurs after the final draft of the policy has been agreed on and, ideally, should also involve other stakeholders, including the private sector and civil society.

[35] Brown, D., & Esterhuysen, E. (2017). *A rights-based approach to cybersecurity: A pipe dream or a critical means to a secure and stable internet?* APC. https://www.apc.org/sites/default/files/IGF17-_A_rights-based_approach_to_cybersecurity_-_recommendations_201807018.pdf; APC. (2020). *APC policy explainer: A human rights-based approach to cybersecurity*. https://www.apc.org/en/pubs/apc-policy-explainer-human-rights-based-approach-cybersecurity

[36] UN Women. (2020). Gender mainstreaming: A global strategy for achieving gender equality and the empowerment of women and girls. https://www.unwomen.org/en/digital-library/publications/2020/04/brochure-gender-mainstreaming-strategy-for-achieving-gender-equality-and-empowerment-of-women-girls

[37] Global Partners Digital. (2022). Op. cit.

Table 3: Core components of cybersecurity policies identified by Global Partners Digital and adapted recommendations developed by APC

	Framing, vision, objectives and definitions	Roles and responsibilities	Cyber resilience
Core components of cybersecurity policies identified by Global Partners Digital framework	This delineates the vision of cybersecurity, the goals and objectives of the cybersecurity policy itself, and definitions of key terms such as "cybersecurity".	This establishes the policy governance mechanisms through the roles and responsibilities of the different actors in cybersecurity.	This sets out a wide range of actions that the government will take to protect infrastructure, networks, systems, information and users from cyber attacks and cyber threats. They can range from cybersecurity exercises and the establishment of CSIRTs to research, training, etc.
Recommendations by APC	In order to have a gender-sensitive cybersecurity policy, the vision of cybersecurity must explicitly recognise the role that cybersecurity plays in protecting people's human rights. As GPD suggests, this should be reflected in the objectives and a definition of cybersecurity consistent with international human rights frameworks. More specifically concerning the gender perspective, progress should at least be made in ensuring that the policy's objectives recognise the differentiated and intersectional security needs of diverse people. Using this framework, and depending on national conditions, concrete and measurable goals can be advanced in the action plan.	A clear and strong commitment to multistakeholder governance is essential for a successful cyber-security strategy. In this context, civil society organisations working on gender and other relevant intersectional issues must be involved in the implementation and review of the policy in order to ensure that a gender approach to cybersecurity policy is properly adopted, and to offer evidence of the success or failure of its adoption.	In addition to the principles of legality and proportionality necessary for the fulfilment of human rights, which are particularly important when considering vulnerabilities due to gender and other intersectionalities, the action plan for building what we call "cyber resilience" can be broad according to national needs. Among the measures that could be contemplated are: • The commitment that the government's critical infrastructure risk models incorporate a gender and intersectional approach to protecting the rights of people given their diverse needs. The government should consider coordinating training sessions with stakeholders on how the gender approach can contribute to developing these models and creating a plan for timely responses to incidents. • Advancing legal and policy frameworks that give legal protection against gender-based cyber threats for women, including journalists and human rights defenders. • Information campaigns: people should have timely and reliable information on digital security, including details of the most common risks they will face. • Equality and diversity: the creation of incentives to ensure that women working in academia, industry and also in the government can pursue STEM careers, be part of the cybersecurity workforce, and be part of cybersecurity policy spaces.

	Cyber incident response	Cybercrime	International cooperation
Core components of cybersecurity policies identified by Global Partners Digital framework	This delineates the broad range of actions the government will take when a cyber attack occurs. For example, it could include developing contingency plans, providing tools and resources to law enforcement agencies, or supporting those affected.	This details how the government will address cybercrime, the development of cybercrime legislation and support for its enforcement.	This details how the government will work with other governments and international and regional organisations on cybersecurity issues (collaboration to address shared threats, promotion of values, foreign policy priorities, etc.).
Recommendations by APC	Cyber incidents must have responses that conform to the principles of legality and proportionality. In addition, among other measures that will depend on national needs, it is possible to propose the following: • Special contingency plans that, based on a gender and intersectionality analysis, seek to protect people most vulnerable to specific types of cyber attacks. • The provision of resources to support the infrastructure of groups identified in your gender and intersectional analysis that have been victims of cyber attacks due to their work.	In addition to definitions of cybercrime being in line with human rights standards, they should, at the very least, involve the following: • A review of legal frameworks and public policies that can respond to the various online gender-based attacks in the local context, such as the intrusion into or disruption of personal devices and networks, doxing, cyberbullying and the non-consensual dissemination of intimate images. • The training of cybercrime police regarding online gender-based violence. • Mandatory collection by the cybercrime police of disaggregated data, including online gender-based attacks, when reporting cybercrime.	International collaboration in cybersecurity should be based on respecting and strengthening human rights and an open, free and secure internet. Likewise, governments should consider cyberspace as a space free of gender-based violence and commit efforts to eradicate it. In addition, international cooperation should focus on the following: • Incorporating gender considerations as an integral part of the debate on cyber threats. • Integrating discussions on the legal aspects of international peace, security and justice to understand the impact of malicious cyber operations on vulnerable groups. • Adopting a multistakeholder approach to building trust, peace and stability in cyberspace. • Working on capacity building with a human-centred approach and integrating a gender perspective.[38]

[38] For more principles that capacity building should follow, consult the Final Substantive Report (2021) from the "Open-ended working group on developments in the field of information and telecommunications in the context of international security": https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

RECOMMENDATIONS

Suggest specific policy texts on gender and cybersecurity:

Propose incorporating specific texts, words and phrases that you have collected in the research phase. While there is no guarantee that the text will remain in the final policy document, it provides a concrete reference point for debate.

Influence implementation and review plans:

Following the development of the policy document, an action plan needs to be developed to implement the policy. This is also an important process that the gender champion needs to try to influence. Key issues to consider here are:

- Suggest who may be the actors in charge of compliance, monitoring, evaluation and review and who have the skills and capacity to take on these responsibilities. Ensure that they understand properly why a gender approach to cybersecurity is necessary. Consider negotiating in advance with stakeholders who may be interested in taking on this responsibility.
- With a possible budget estimate, propose concrete actions with measurable short-, medium- and long-term goals. As in any budget, the activities with the lowest cost for the government may have a better chance of being priorities.
- Formulate actions built on infrastructure or programmes already implemented by the government or other stakeholders. The continuity of these activities or strengthening them can be an excellent excuse to prioritise them.

At the formative stage, the most critical aspect of the action plan is the availability of adequate resources for the implementation of the policy, and for setting up mechanisms for monitoring and review.

The action plan should be considered a strategic area of intervention because it is where the commitments included in the national cybersecurity policy have a real possibility of going from being just words to reality. This is particularly important as there could be a temptation to only include gender in the policy for publicity purposes.

c. International engagement aspect

In the start-up stage, you would have already mapped your government's engagement in global cybersecurity forums, and determined whether or not and to what extent gender issues are foregrounded in these discussions. Here you may want to revisit this mapping to see if any adjustments need to be made. Based on what you have determined regarding your government's knowledge about a gender approach to cybersecurity and how this translates into its engagement in international forums, you may want to consider various capacity-building measures for government delegates, including meetings, training sessions and seminars on gender and cybersecurity, and international cooperation to initiate or deepen knowledge on the subject.

RECOMMENDATION

Build the confidence of policy makers to engage in international forums:

Based on your mapping of cybersecurity forums in the start-up phase, build the capacity of designated policy makers so that they can participate meaningfully in these forums. Many of these forums have online engagement mechanisms, but a budget may need to be set aside for in-person attendance. It is highly recommended that first-time attendees seek a mentor, possibly a civil society organisation, to introduce them to the forum's mechanisms and processes.

C. ESTABLISHED STAGE

The national cybersecurity strategy and its action plan are already in place at the established stage. The most critical objective now is to actively participate in evaluating the impact of the policy as well as your government's performance in international forums and mechanisms for bilateral or multilateral cooperation.

a. Strategy development aspect

At this stage, monitoring and evaluation of the policy should be underway based on compliance with the action plan. There are two possible cases: one in which the policy implemented incorporates gender to varying degrees, and the other in which it does not. In both cases, policy makers and other stakeholders should gather concrete evidence to review how the policy and its action plan have responded to the cybersecurity challenges in the context of gender.

Then, a diagnostic report that clearly shows the gaps and suggests ways to remedy these should be developed and submitted to the monitoring and evaluation mechanisms. This can be complemented with other presentations to stakeholders for purposes of transparency.

In addition to submitting evidence to the mechanisms, other awareness-raising actions could be evaluated. For more on this, review the start-up stage in this document, particularly the strategy development section.

RECOMMENDATION

Encourage a continuous cycle of evaluation and review:

At this stage, monitoring and evaluation of the policy should be underway based on compliance with the action plan. Policy makers and other stakeholders should gather concrete evidence to review how the policy and its action plan have responded to the cybersecurity challenges. A review of the policy should clearly identify gaps in the text of the policy or in its implementation and have a concrete action plan on how to address these gaps. A continuous cycle of monitoring and review should be built into the implementation plan.

b. Content/implementation and review aspects

The national cybersecurity strategy should incorporate and/or support broader policy objectives, such as child protection, promotion of human rights, combating disinformation, and promotion of equality, diversity and digital inclusion, among others. It is vital to create opportunities for dialogue, knowledge sharing and cooperation between government bodies who have an interest in a gender approach to cybersecurity to understand whether the policy is being effective from their perspective.

RECOMMENDATION

Build cross-sectoral cooperation and dialogue between government departments and officials:

The national cybersecurity strategy should incorporate and/or support broader policy objectives, such as child protection, digital inclusion, the promotion of human rights, equality and diversity, and combating disinformation. Develop strategies and processes to ensure that officials working in these areas discuss issues and challenges they may be facing, and share key learnings in the implementation of the policy and its impact on their work.

c. International engagement aspect

At this stage, the country's engagement in regional and international forums is much more active. It is important to create opportunities for collaboration between different stakeholders in these forums, including government, civil society and business, so that a common front on the issue of gender and cybersecurity is presented.

RECOMMENDATION

Work together with different stakeholders to create a common front in international forums:

At this stage, the country's engagement in regional and international forums is much more active. However, there are many power dynamics at play in these forums, with the perspectives of countries in the global South often marginalised by the more powerful nations. Policy makers should consider working with civil society and business groups committed to a gender approach to cybersecurity in order to strengthen their voices at these forums.

D. OTHER STAGES: STRATEGIC AND DYNAMIC

In these two stages, all stakeholders should consider the gender perspective in cybersecurity as a strategic and critical tool, at least for:

- Regularly assessing the damage that cybersecurity incidents can cause differentially to individuals.
- Making cybersecurity risk assessments more complete, nuanced and diverse.
- Re-evaluating and ultimately, if needed, making changes to approaches so that the policy and practice can address the effects of cyber threats more comprehensively.
- Assessing and strengthening diversity in the cybersecurity industry.

In this way, the gender perspective in cybersecurity has a tangible impact on developing a robust and resilient infrastructure to prevent attacks, strengthening human rights for the diversity of people in cyberspace, and creating a resilient cybersecurity culture in society and in corporations.

These factors will help the country to become a champion of a gender approach to cybersecurity policy development in regional and international forums, with its policy serving as a model that can be used by others.

APC
ASSOCIATION FOR
PROGRESSIVE
COMMUNICATIONS

A FRAMEWORK FOR DEVELOPING
GENDER-RESPONSIVE CYBERSECURITY
POLICY: ASSESSMENT TOOL