A FRAMEWORK FOR DEVELOPING GENDER-RESPONSIVE CYBERSECURITY POLICY

NORMS, STANDARDS AND GUIDELINES

A framework for developing gender-responsive cybersecurity policy: Norms, standards and guidelines

This publication was developed and produced by APC. External researcher Paz Peña was the author.

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

Editorial support: Gaurav Jain (APC)

Copy editing and proofreading: Lori Nordstrom (APC)

Design and layout: Cathy Chen (APC)

Published by APC 2022

ISBN 978-92-95113-54-1
APC-202212-GAPS-R-EN-DIGITAL-344

This publication was developed with support from the UK Government.

THE CONVENTION ON THE ELIMINATION OF ALL FORMS OF DISCRIMINATION AGAINST WOMEN (CEDAW)

BEIJING DECLARATION AND PLATFORM FOR ACTION

WOMEN, PEACE AND SECURITY (WPS) AGENDA, AS ESTABLISHED BY UN SECURITY COUNCIL RESOLUTION 1325 AND THE WPS NATIONAL ACTION PLANS

OUTCOME DOCUMENTS OF THE WORLD SUMMIT ON THE INFORMATION SOCIETY (WSIS)

THE 2030 AGENDA FOR SUSTAINABLE DEVELOPMENT AND THE SUSTAINABLE DEVELOPMENT GOALS

UN HUMAN RIGHTS COUNCIL (HRC) REPORTS AND RESOLUTIONS

INTERNATIONAL TELECOMMUNICATION UNION (ITU) INITIATIVES

UN SYSTEM CYBERSECURITY PROCESSES

INTRODUCTION

While great strides have been made in recognising the applicability of human rights frameworks to gender-based threats and abuses in digital contexts, the gendered impact of international cyber operations and incidents, as well as gender inequality, has been a largely unexplored part of the discourse in more securitised cyber processes and forums.

In this context, there are relevant tools, agendas and frameworks that cybersecurity policy makers can draw upon when seeking to promote a gender perspective within local or multilateral cybersecurity. According to Brown and Pytlak, they can be used as a source of information or to establish policy coherence with states' existing commitments to gender equality.[1]

This paper, which forms part of a framework developed by the Association for Progressive Communications to promote gender-responsive cybersecurity policy, presents an overview of the most relevant of these instruments.

1. Brown, D., & Pytlak, A. (2020). *Why Gender Matters in International Cyber Security*. Women's International League for Peace and Freedom and the Association for Progressive Communications. https://www.apc.org/en/node/36261

THE CONVENTION ON THE ELIMINATION OF ALL FORMS OF DISCRIMINATION AGAINST WOMEN (CEDAW)

Adopted by the United Nations General Assembly in 1971, the Convention on the Elimination of all Forms of Discrimination against Women (CEDAW)[2] begins by recognising that widespread discrimination against women violates the principles of equal rights and respect for human dignity. In this context, this is the first international instrument that extends state responsibility to acts committed by private persons, companies, non-state institutions or non-governmental organisations. Article 2(e) establishes that states are obliged to "take all appropriate measures to eliminate discrimination against women by any person, organization or enterprise."[3]

The Committee on the Elimination of Discrimination against Women monitors the fulfilment of obligations by states parties to the Convention, which numbered 189 as of 2020. States parties must submit a report every four years, which is discussed at an annual session. The Committee may also issue general recommendations, which serve as authoritative interpretations of the articles of the Convention. Brown and Pytlak enumerate various ways in which general recommendations adopted by the Committee in recent years have taken information and communications technologies (ICTs) into account.[4] For instance:

- General recommendation No. 35 on "gender-based violence against women, updating general recommendation No. 19" includes in its updated understanding of gender-based violence against women the "redefinition through technology-mediated environments, such as contemporary forms of violence occurring on the Internet and digital spaces."[5]
- General recommendation No. 36 "on the right of girls and women to education" recognises the under-representation of girls and women "in the use of information and communication technology (ICT) skills" and further calls on schools to address barriers to accessing information and employment opportunities in relevant industries.[6]
- To the above, we can add the more recent General recommendation No.38 on "trafficking in women and girls in the context of global migration". Specifically, its section E on "Use of digital technology in trafficking" acknowledges that while there is a positive impact of technologies on society, they also pose "new security challenges at both the individual and State levels." In particular, "[t]he use of electronic currencies offers tools for hiding personal information, such as the identification of the parties involved in the transaction and their location, and allow for making anonymous payments, without even disclosing the purpose of the transaction, all of which facilitates trafficking. Demand channels, through social media, the dark web and messaging platforms, provide easy access to potential victims, thereby increasing their vulnerability."[7]

2. https://www.un.org/womenwatch/daw/cedaw/text/econvention.htm
3. Ibid.
4. Brown, D., & Pytlak, A. (2020). Op. cit.
5. CEDAW/C/GC/35. https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_35_8267_E.pdf
6. CEDAW/C/GC/36. https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_36_8422_E.pdf
7. CEDAW/C/GC/38. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-recommendation-no38-2020-trafficking-women

CEDAW and the Women, Peace and Security (WPS) Agenda

According to Myrttinen, the synergy between CEDAW and Resolution 1325 inaugurating the WPS Agenda (studied in greater depth later in this paper) is emphasised by CEDAW recommendation 30 on "women in conflict prevention, conflict and post-conflict situations", in which the CEDAW Committee links the implementation of the Resolution to the CEDAW reporting mechanisms.[8]

8. Myrttinen, H. (2020). *Tool 1: Security Sector Governance, Security Sector Reform and Gender.* DCAF, OSCE/ODIHR & UN Women. https://www.dcaf.ch/tool-1-security-sector-governance-security-sector-reform-and-gender

BEIJING DECLARATION AND PLATFORM FOR ACTION

The Beijing Declaration and Platform for Action[9] was adopted by the states participating in the UN Fourth World Conference on Women in 1995. It was negotiated with significant input from civil society and, according to UN Women itself, is considered "the most progressive blueprint ever for advancing women's rights."[10] The Platform for Action is organised into 12 areas of particular concern, and several of them can be related to gender and cybersecurity, even though the issue is not directly addressed.

Section E: Women and armed conflict

This section criticises excessive military spending and calls for a gender perspective in these expenditures. It states, for example:

- Paragraph 138: Those affected most negatively by conflict and excessive military spending are people living in poverty, who are deprived because of the lack of investment in basic services.
- Paragraph 141: In addressing armed or other conflicts, an active and visible policy of mainstreaming a gender perspective into all policies and programmes should be promoted so that before decisions are taken an analysis is made of the effects on women and men, respectively.

Strategic objective E.2 outlines various actions to reduce excessive military expenditures and control the availability of armaments.

Section J: Women and the media

This section refers to the role of the media in the well-being of women and explicitly considers new information and communications technologies. Thus, for example, it recognises that:

- Paragraph 234: During the past decade, advances in information technology have facilitated a global communications network that transcends national boundaries and has an impact on public policy, private attitudes and behaviour, especially of children and young adults. Everywhere the potential exists for the media to make a far greater contribution to the advancement of women.
- Paragraph 236: The continued projection of negative and degrading images of women in media communications – electronic, print, visual and audio – must be changed. Print and electronic media in most countries do not provide a balanced picture of women's diverse lives and contributions to society in a changing world.
- Paragraph 237: Women [...] need to be involved in decision-making regarding the development of the new technologies in order to participate fully in their growth and impact.

One of Section J's strategic objectives in particular addresses the relationship between gender and digital technologies: Strategic objective J.1, which calls for increasing "the participation and access of women to expression and decision-making in and through the media and new technologies of communication." The measures suggested to governments to meet this objective that are of interest to the cybersecurity agenda include the following:

9. https://www.un.org/womenwatch/daw/beijing/pdf/BDPfA%20E.pdf
10. https://www.unwomen.org/en/digital-library/publications/2015/01/beijing-declaration

- Encourage and recognize women's media networks, including electronic networks and other new technologies of communication, as a means for the dissemination of information and the exchange of views, including at the international level, and support women's groups active in all media work and systems of communications to that end.
- Encourage the development of educational and training programmes for women in order to produce information for the mass media, including funding of experimental efforts, and the use of the new technologies of communication, cybernetics space and satellite, whether public or private.
- Encourage the use of communication systems, including new technologies, as a means of strengthening women's participation in democratic processes.

Beijing Declaration and Sustainable Development Goals

In 2020, UN Women published a review of women's rights 25 years after the Beijing Declaration and linked the 12 critical areas of the Beijing Platform for Action with the 17 Sustainable Development Goals, highlighting four universal catalysts for change, among which "Harnessing technology for gender equality" stands out. It recognises the enormous potential of new technologies for the empowerment of women and girls but warns that it is essential to close the gender digital divide first, as well as to eliminate new risks such as cyber violence, threats to the right to privacy, or algorithms that perpetuate unconscious bias.[11]

11. UN Women. (2020, 9 March). Opening statement by Under-Secretary-General of the United Nations and Executive Director of UN Women, Phumzile Mlambo-Ngcuka, at the 64th session of the Commission on the Status of Women 9 March 2020. https://www.unwomen.org/en/news/stories/2020/3/speech-ed-phumzile-csw64

WOMEN, PEACE AND SECURITY (WPS) AGENDA, AS ESTABLISHED BY UN SECURITY COUNCIL RESOLUTION 1325 AND THE WPS NATIONAL ACTION PLANS

In October 2000, the WPS Agenda was established by United Nations Security Council Resolution 1325, which applies to all UN members. The resolution moves away from viewing women only as victims and affirms the critical role of women in conflict prevention and resolution, peacekeeping, peacebuilding, humanitarian response, and post-conflict reconstruction, and urges states to increase women's participation in all UN peace and security work, including security-related decision making. The WPS Agenda is thus based on the principle that effective gender mainstreaming and women's rights can have a significant and positive impact on the lives of women, men, girls and boys on the ground.

Since the resolution embodies the essential principles of equality and non-discrimination, it reinforces the human rights standards established by international instruments, including, in particular, the Convention on the Elimination of All Forms of Discrimination against Women.

That initial resolution in 2000 has been followed by nine other WPS resolutions, which together form the basis of its agenda. However, none of the resolutions contains references to "cyber", "online", "technology", "digital" or "internet", nor to cyberspace or cybersecurity; and where there have been indirect references, these have tended to focus on two aspects: the use of ICTs to enable women's rights and political participation, and the use of ICTs to abuse or perpetrate violence against women.[12]

The WPS Agenda has four pillars: participation, protection, prevention (these first three are known as the "three Ps"), and relief and recovery. To implement the WPS Agenda, there are National Action Plans (NAPs) and Regional Action Plans (RAPs). Only two NAPs mention cyber threats: the 2019 NAPs of Ireland and Namibia.[13]

12. Sharland, L., et al. (2021). *System Update: Towards a Women, Peace and Cybersecurity Agenda*. UNIDIR. https://doi.org/10.37559/GEN/2021/03
13. Ibid.

Opportunities for the WPS Agenda and cybersecurity

According to Brown and Pytlak, there has been insufficient examination of how the WPS Agenda or NAPs could be integrated or leveraged in international cybersecurity policy discussions.[14] However, given the legally binding nature of UN Security Council resolutions for all member states, it could inform efforts to close the gender digital divide and provide better online protection.

More specifically, Sharland et al. propose that in order to bridge the gap between the WPS Agenda and cybersecurity and update international security to the 21st century, six challenges need to be addressed in this Agenda:

1. Women's participation in cybersecurity negotiations

The WPS Agenda seeks to achieve the effective and meaningful participation of women across the entire spectrum of international security, including international negotiations and decision making on cyber issues. In this regard, one of the most identifiable challenges is to increase the participation of women in international cybersecurity decision making. Moreover, it is a priority to actively incorporate gender perspectives into policies and programmes that complement these efforts.

2. Cyber violence against women and girls

Protecting women and girls from cyber violence is an integral part of the WPS Agenda and should be included in NAPs and RAPs to implement Resolution 1325. This will require states to adjust how they address issues traditionally framed as a domestic concern (e.g. the human harms of cyber violence) in NAPs on women, peace and security, rather than focusing only on external security threats.

3. Women's participation in political processes

Women's participation in politics and government institutions is critical to efforts to strengthen women's representation and amplify their voices, thus advancing efforts to enhance the agenda of women and children. However, the ease with which ICTs allow women to be intimidated and harassed increases barriers to their participation in political processes.

4. Gender and online radicalisation

The use of the internet to spread ideology and radicalise individuals has exponentially increased the pool of extremist organisations. However, the gendered influences and impacts of far-right rhetoric online remain largely unexplored in the literature and state debates. Understanding the different appeal of these platforms and the gendered engagement with them is key to addressing some of the risks they present to peace and security to prevent and respond to the radicalisation of individuals through these platforms.

14. Brown, D., & Pytlak, A. (2020). Op. cit.

5. Gendered impacts of cyber incidents

More research is needed to examine the gender-differentiated impact of cybersecurity policy instruments (such as internet shutdowns), data breaches, and attacks on critical infrastructure. States should also seek to incorporate a gender perspective in developing their policies around critical infrastructure protection, including framing and defining what constitutes "critical infrastructure" and "critical information infrastructure" and the priority assigned to different types of incidents.

6. Gender bias in digital technologies

Research has shown that threat model, user notification and control procedures and the advertising of cybersecurity technologies make women more likely to have cybersecurity threats minimised or omitted. Ensuring diversity in cyber and artificial intelligence (AI) workforces and processes and integrating a gender perspective into cyber and AI initiatives, materials and training programmes are possibilities to address the problem.[15]

15. Sharland, L., et al. (2021). Op. cit.

OUTCOME DOCUMENTS OF THE WORLD SUMMIT ON THE INFORMATION SOCIETY (WSIS)

The World Summit on the Information Society (WSIS) process consisted of two United Nations-sponsored conferences addressing information, communications and the information society. It was organised in two phases: Geneva in 2003 and Tunis in 2005. One of its most important objectives was to help bridge the digital divide between developing and developed countries by increasing access to modern ICT services.

The following paragraphs of the Geneva Declaration of Principles (the outcome document of the first phase),[16] which was supported by UN member states and all stakeholders, are of particular interest here:

- 12. We affirm that development of ICTs provides enormous opportunities for women, who should be an integral part of, and key actors, in the Information Society. We are committed to ensuring that the Information Society enables women's empowerment and their full participation on the basis of equality in all spheres of society and in all decision-making processes. To this end, we should mainstream a gender equality perspective and use ICTs as a tool to that end.
- 13. In building the Information Society, we shall pay particular attention to the special needs of marginalized and vulnerable groups of society, including migrants, internally displaced persons and refugees, unemployed and underprivileged people, minorities and nomadic people. We shall also recognize the special needs of older persons and persons with disabilities.

The Tunis Commitment (adopted during the second phase)[17] recognises the gender gap and reaffirms the commitment of all stakeholders to promote the participation of women in decision-making processes. The following paragraphs are particularly relevant:

- 13. We also recognize that the ICT revolution can have a tremendous positive impact as an instrument of sustainable development. In addition, an appropriate enabling environment at national and international levels could prevent increasing social and economic divisions, and the widening of the gap between rich and poor countries, regions, and individuals – including between men and women.
- 23. We recognize that a gender divide exists as part of the digital divide in society and we reaffirm our commitment to women's empowerment and to a gender equality perspective, so that we can overcome this divide. We further acknowledge that the full participation of women in the Information Society is necessary to ensure the inclusiveness and respect for human rights within the Information Society. We encourage all stakeholders to support women's participation in decision-making processes and to contribute to shaping all spheres of the Information Society at international, regional and national levels.

The text also recognises that the international community should pay special attention to marginalised and vulnerable groups' unique needs in society.

16. WSIS-03/GENEVA/DOC/4-E. https://www.itu.int/net/wsis/docs/geneva/official/dop.html
17. WSIS-05/TUNIS/DOC/7-E. https://www.itu.int/net/wsis/docs2/tunis/off/7.html

Resolution 70/125: Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society

In 2015, when the World Summit on the Information Society went through a 10-year review, the UN General Assembly adopted Resolution 70/125,[18] which expresses concern about the persistence of the digital divide between males and females, and states: "We encourage all stakeholders to ensure the full participation of women in the information society and women's access to new technologies, especially information and communications technologies for development."

It further notes that, in the context of the unique and emerging challenges concerning technologies that have been emerging in the countries, "[p]articular attention should also be paid to addressing the specific information and communications technology challenges facing children, youth, persons with disabilities, older persons, indigenous peoples, refugees and internally displaced persons, migrants and remote and rural communities."

More specifically, the resolution called for "immediate measures to achieve gender equality in Internet users by 2020, especially by significantly enhancing women's and girls' education and participation in information and communications technologies, as users, content creators, employees, entrepreneurs, innovators and leaders. We reaffirm our commitment to ensure women's full participation in decision-making processes related to information and communications technologies."

18. A/RES/70/125. https://unctad.org/system/files/official-document/ares70d125_en.pdf

THE 2030 AGENDA FOR SUSTAINABLE DEVELOPMENT AND THE SUSTAINABLE DEVELOPMENT GOALS

The 2030 Agenda for Sustainable Development is a comprehensive and interdependent approach to sustainable socioeconomic development that builds on previous multilateral processes and agreements. The 17 Sustainable Development Goals (SDGs) are the main mechanisms of the 2030 Agenda, adopted on 25 September 2015 by the United Nations General Assembly (UNGA) in resolution A/RES/70/1: "Transforming our world: the 2030 Agenda for Sustainable Development".[19]

Of particular interest here is SDG 5, which aims to "achieve gender equality and empower all women and girls." Like all the Goals, SDG 5 has a set of specific targets and corresponding indicators, some of which are particularly relevant to the field of cybersecurity:

- 5.1 End all forms of discrimination against all women and girls everywhere.
- 5.2 Eliminate all forms of violence against all women and girls in the public and private spheres, including trafficking and sexual and other types of exploitation.
- 5.5 Ensure women's full and effective participation and equal opportunities for leadership at all levels of decision-making in political, economic and public life.
- 5.b Enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women.

UNGA Resolution 70/25 (adopted by the General Assembly at the WSIS 10-year review on 16 December 2015)[20] also states:

> We recognize that ending the gender digital divide and the achievement of Sustainable Development Goal 5 on gender are mutually reinforcing efforts, and we commit to mainstreaming gender in the World Summit on the Information Society process, including through a new emphasis on gender in the implementation and monitoring of the action lines, with the support of relevant United Nations entities, including the United Nations Entity for Gender Equality and the Empowerment of Women (UN-Women).

According to a report published by the think tank New America, although the literature on the subject is still in its infancy, cybersecurity plays a vital role in this goal, as inequalities in this field exacerbate existing social inequalities such as those based on gender.[21] In addition, online resources for reporting discrimination and violence against women require strict privacy controls or risk putting women at greater risk.

19. A/RES/70/1. https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_70_1_E.pdf
20. A/RES/70/125. https://unctad.org/system/files/official-document/ares70d125_en.pdf
21. Morgus, R. (2018). *Securing Digital Dividends. Mainstreaming Cybersecurity in International Development*. New America. https://www.newamerica.org/cybersecurity-initiative/reports/securing-digital-dividends

The International Telecommunication Union's interpretation of SDG 5

The International Telecommunication Union (ITU) has focused considerable efforts on bridging the multiple gaps that women experience in technology.[22] It has done so primarily by encouraging women's and girls' participation in science, technology, engineering and mathematics (STEM) careers and by being part of EQUALS, an innovative global network to build an evidence base and improve women's access to technology, build digital and other skills, and promote women's leadership in the technology sector (APC is also part of EQUALS). For instance, in 2021, the ITU organised the first edition of the Women in Cyber Mentorship Programme targeted at building the capacity of junior women professionals who wish to enter or thrive in the field of cybersecurity.[23]

22. https://www.itu.int/en/mediacentre/backgrounders/Pages/icts-to-achieve-the-united-nations-sustainable-development-goals.aspx
23. ITU. (2021). *ITU Contribution to the Implementation of the WSIS Outcomes: 2021*. Draft as of 25/10/2021. https://www.itu.int/en/itu-wsis/Documents/ITUContribution/2021_ITU_Contribution_to_WSIS-Implementation-20211025.pdf

UN HUMAN RIGHTS COUNCIL (HRC) REPORTS AND RESOLUTIONS

A/HRC/38/47: Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective

In 2018, the UN Special Rapporteur on violence against women, its causes and consequences published a special report on online gender-based violence,[24] which made a decided advance in the definition of the phenomenon and its analysis. It also makes a series of recommendations, among which there are several related to cybersecurity, such as:

- 100. States should ensure that effective measures are taken to prevent the publication of harmful material that comprises gender-based violence against women, and for their removal on an urgent basis. States should adopt, or adapt (as appropriate) their criminal and civil causes of action to hold perpetrators liable. Such legislative measures should be applicable also to threats of releasing harmful information or content online.
- 105. States should provide training for magistrates, lawyers, police and all other law enforcement officials and frontline workers to ensure their ability to investigate and prosecute perpetrators, and foster public trust in obtaining justice for cases of online and ICT-facilitated violence.
- 107. States should provide protective measures and services for victims of online gender-based violence; this includes specialized helplines to provide support to those who have been attacked online, shelters and protection orders.
- 110. States should provide education, outreach and gender-sensitive training for Internet users on online and ICT-facilitated violence against women and girls in schools and communities as a way to prevent it.
- 112. States should guarantee the enforcement of strong data protection regulations and ensure the accountability of data holders in cases of breach.
- 113. States should protect and encourage the development of technology, including of encryption and anonymity tools that protect the rights and security of women online.

Recommendations for internet intermediaries related to cybersecurity include the following:

- 118. Intermediaries should ensure data security and privacy, and ensure that the use of data is in compliance with international human rights law and has the fully informed consent of data providers.
- 119. Internet platforms should commit to eradicating online gender-based violence. In this sense, they should allocate resources to information and education campaigns on preventing ICT-facilitated violence against women and girls and on promoting human rights and digital security.

A/HRC/RES/38/5: Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts

In 2018, the UN Human Rights Council adopted a resolution led by Canada and with the consensus of more than 50 co-sponsors from all regions, stating that online gender-based violence is a human rights violation "which hinders their full, equal and effective participation in

24. A/HRC/38/47. https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violence-against-women-its-causes-and

economic, social, cultural and political affairs and is an impediment to achieving gender equality and the empowerment of all women and girls."[25]

Actions recommended to states include the following:

> Prioritizing the integration of gender perspectives, and ensuring the early, full and effective participation of women and girls in the development and implementation of national policies, legislation, programmes, projects, strategies and regulatory and technical instruments in the area of digital technologies and creating monitoring and accountability mechanisms to ensure implementation of gender-sensitive policies and regulations, as well as analysing the gender impact of such policies in consultation and collaboration with women digital technology specialists, civil society organizations and gender equality advocates.

The resolution also urges states to call on private actors working in digital technologies to adopt a series of actions to end this type of violence, including the incorporation of a gender perspective in the design, development and application of technologies.

25. A/HRC/RES/38/5. https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/38/5

INTERNATIONAL TELECOMMUNICATION UNION (ITU) INITIATIVES

Resolution 70: Mainstreaming a gender perspective in ITU and promotion of gender equality and the empowerment of women through telecommunications/information and communication technologies

At their 2018 Plenipotentiary Meeting, ITU member states adopted Resolution 70, "Mainstreaming a gender perspective in ITU and promotion of gender equality and the empowerment of women through telecommunications/information and communication technologies".[26]

Among other things, it recognises that:

- Equal access to ICTs and equal participation at all levels and in all areas, especially in policy and decision making, are beneficial to society as a whole.
- Bridging the gender digital divide requires the promotion of digital skills, education and mentoring of women and girls to advance their participation and leadership in the creation, development and deployment of telecommunications/ICTs.
- There is a need to further encourage the participation of women and girls in the telecommunication/ICT field at an early age and provide information for developing new policies.

The resolution includes a series of commitments for measures to mainstream a gender perspective and advance gender equality within the ITU itself, and commits ITU member states to a series of actions concerning:

- Employment, training and promotion
- Facilitating capacity building
- Reviewing policies and strategies
- Attracting more women and girls into STEM careers and recognising the success of those already in the field.

The 2022 Guidelines for utilization of the Global Cybersecurity Agenda (GCA)

Launched in 2007, the Global Cybersecurity Agenda (GCA)[27] is an international cooperation framework aimed at improving trust and security in the information society. The GCA is designed for cooperation and efficiency, fostering collaboration with and among all relevant partners, and building on existing initiatives to avoid duplication of efforts. It is built upon five strategic pillars: legal measures, technical and procedural measures, organisational structures, capacity building and international cooperation. The GCA is the basis used by the ITU to publish its Global Cybersecurity Index (GCI),[28] to shed more light on countries' cybersecurity commitments. Each country's level of development or engagement is assessed based on the five pillars of the GCA.

26. Resolution 70 (Rev. Dubai, 2018). https://www.itu.int/en/ITU-D/Digital-Inclusion/Documents/Resolutions/RESOLUTION%2070%20(REV.%20DUBAI,%202018).pdf
27. https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx
28. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
29. https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx

In 2021, the ITU published the latest draft guidelines on how the organisation itself uses the GCA,[29] and in March 2022, ITU Council member states approved the documents for transmission to the 2022 ITU Plenipotentiary Conference. Among these is the "Draft information document for guidelines for utilization of the Global Cybersecurity Agenda",[30] which recognises that many ICT end users do not fully understand cybersecurity issues or have the skills or tools needed to protect their data, privacy and assets. The most vulnerable users, including women and children, are particularly exposed to risk. Therefore, building skills, competencies and measures to achieve an effective cybersecurity culture remains a crucial challenge.

Within the framework of this diagnosis, some suggestions are made regarding gender under the pillar of capacity building:

- 5.3 It is important to note also that, given the rapid advancements in ICTs and the already existing issues of access and connectivity, end users – and in particular populations such as women, children, older persons, persons with disabilities and specific needs – can often be more vulnerable to cybersecurity threats and incidents. Cybersecurity-related education programmes, in addition to raising awareness about cybersecurity threats relevant to vulnerable end users, could therefore be key to decreasing cybersecurity risks for society as a whole.
- 5.11 Further, from a global perspective, empowering human resources requires a general, modular and flexible cybersecurity educational framework to respond to the needs of increased public awareness, and to provide tailored educational curricula for specific professionals. Particular attention should be paid to the gender gap in this area. There is a lot of untapped human capital that can be brought to contribute to the cybersecurity field, including women who still represent only 20% of the cybersecurity workforce.

In particular, in capacity building, the ITU pledges to pay special attention to the needs of the most vulnerable groups, such as women, children, older persons, and persons with disabilities and specific needs.

Guide to Developing a National Cybersecurity Strategy

To reap the benefits and manage the challenges of digitisation, countries must frame their digital transformation and the proliferation of ICT-based infrastructure and services within a comprehensive National Cybersecurity Strategy (NCS).

To support governments in this effort, a consortium of partner organisations from the public and private sectors, civil society and academia, facilitated by the ITU, jointly developed and published a guide to developing a national cybersecurity strategy in 2018.[31] The 2021 version of the guide[32] updates, refines, clarifies and expands on that earlier version.

As cybersecurity affects many areas of socioeconomic development and is influenced by numerous factors within the national context, section 5 of the 2021 guide, "National Cybersecurity Strategy Good Practice", introduces a set of good-practice elements that can make the Strategy comprehensive and effective, while allowing for tailoring to the national context.

30. https://www.itu.int/md/S22-CL-INF-0008/en
31. https://www.itu.int/pub/D-STR-CYB_GUIDE.01
32. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf

While there are references to gender, they are again made within the framework of "capability and capacity building and awareness raising". For instance, the guide recommends that:

- The Strategy should also foster initiatives that aim to develop dedicated cybersecurity career paths and an effective pipeline of future employees, in particular for the public sector, and promote incentives to increase the supply of qualified cybersecurity professionals and help retain talent. These should be created in partnership with academia, the private sector, and civil society. To address the ongoing gender gap of experts in cybersecurity, a gender-balanced approach that motivates, encourages, and facilitates more engagement from women should be considered across all efforts aimed at skills-development and training, ensuring inclusivity in the future.
- The Strategy should identify those groups of society which require particular attention when it comes to cybersecurity capacity and capability building and awareness raising. These include groups which have been identified as being particularly at risk or which need to be empowered to protect themselves, such as small and medium enterprises (SMEs), community-based organisations (CBOs), underserved communities, and/or low-income communities.

UN SYSTEM CYBERSECURITY PROCESSES

At the UN General Assembly's First Committee, two processes – the UN Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG) – have been exploring the same question: responsible state behaviour in cyberspace.

Group of Governmental Experts (GGE)

General Assembly resolution 73/266, "Advancing responsible state behaviour in cyberspace in the context of international security", adopted in December 2018, mandated the creation of a new iteration of the Group of Governmental Experts to continue to study how international law applies to state action in cyberspace, among other objectives.[33] Accordingly, between 2019 and 2021, the GGE continued its work to promote common understandings and effective implementation of possible cooperative measures to address existing and potential threats in the sphere of information security. Its 2021 report[34] contains the Group's findings on existing and emerging threats; norms, rules and principles for the responsible behaviour of states; international law; confidence-building measures; and international cooperation and assistance in ICT security and capacity building.

In the document's section on "Norms, rules and principles for the responsible behaviour of States", the GGE establishes in Norm 13 (e):

> States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

The norm explainer specifically refers to gender as a way to contribute to non-discrimination:

- 36. This norm reminds States to respect and protect human rights and fundamental freedoms, both online and offline in accordance with their respective obligations. Requiring special attention in this regard is the right to freedom of expression including the freedom to seek, receive and impart information regardless of frontiers and through any media, and other relevant provisions provided for in the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and as set out in the Universal Declaration of Human Rights. Observance of this norm can also contribute to promoting non -discrimination and narrowing the digital divide, including with regard to gender.
- 40. While recognizing the importance of technological innovation to all States, new and emerging technologies may also have important human rights and ICT security implications. To address this, States may consider investing in and advancing technical and legal measures to guide the development and use of ICTs in a manner that is more inclusive and accessible and does not negatively impact members of individual communities or groups.

33. Brown, D. (2019, 10 January). UN General Assembly adopts record number of resolutions on internet governance and policy: Mixed outcomes for human rights online. *APC*. https://www.apc.org/en/node/35253
34. https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

- 41. The Group notes that within the United Nations a number of dedicated fora specifically address human rights issues. In addition, it acknowledges that a variety of stakeholders contribute in different ways to the protection and promotion of human rights and fundamental freedoms online and offline. Engaging these voices in policy-making processes relevant to ICT security can support efforts for the promotion, protection and enjoyment of human rights online and help clarify and minimise potential negative impacts of policies on people, including those in vulnerable situations.

Open-ended Working Group (OEWG)

Under UN General Assembly Resolution 73/27, an Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) was established in which all UN member states were invited to participate. The Group met for the first time in 2019 and published its final report in 2021.[35]

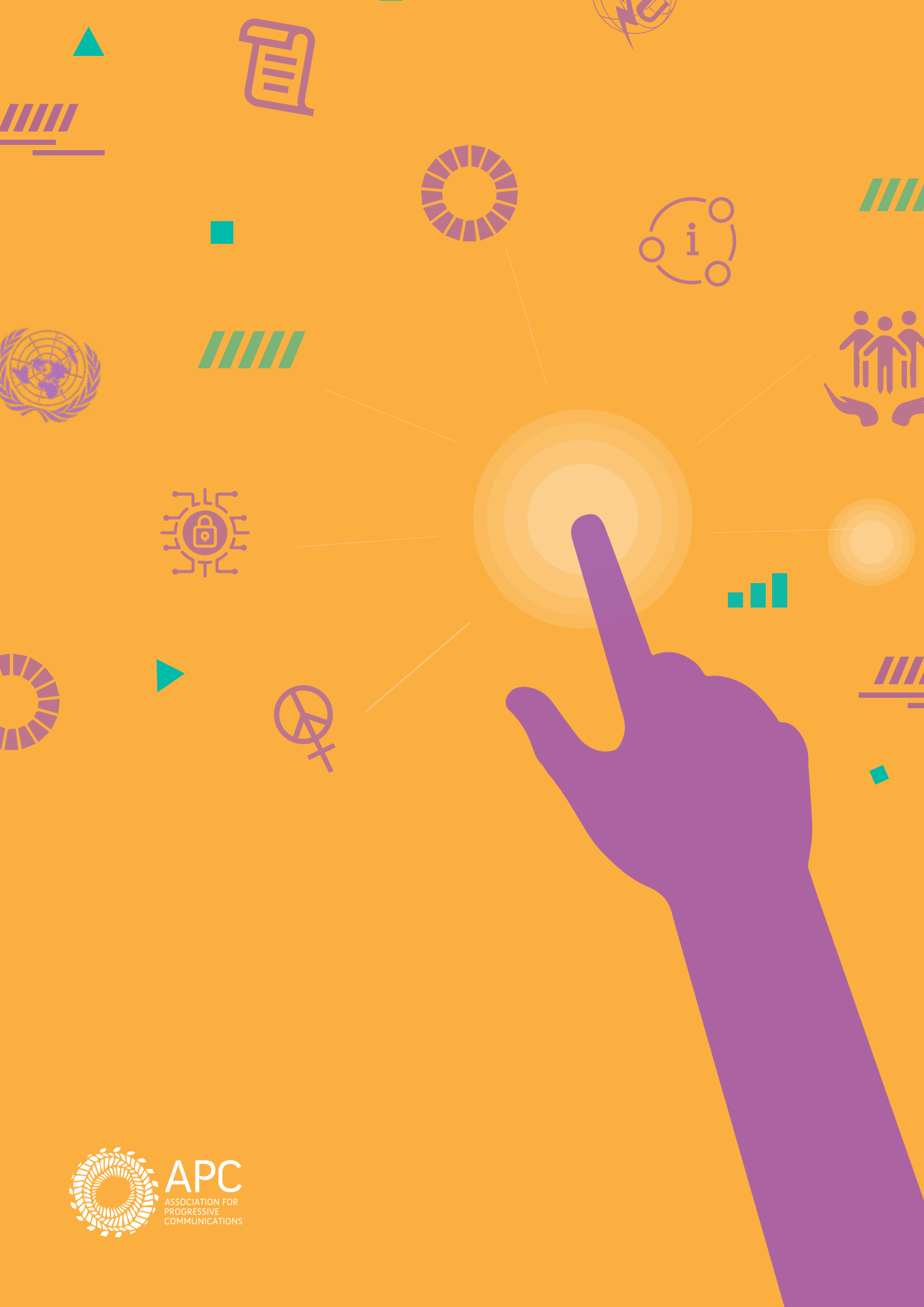
In that report, the OEWG welcomed the high level of participation of women delegates in its sessions and the importance of gender perspectives in its discussions. Moreover, its introduction stresses the importance of reducing the "gender digital divide" and promoting effective and meaningful participation and leadership of women in decision-making processes related to the use of ICTs in the context of international security. However, despite this, the conclusions and recommendations are very limited with regard to consideration of gender:

- 21. States concluded that threats may be experienced differently by States according to their levels of digitalization, capacity, ICT security and resilience, infrastructure and development. Threats may also have a different impact on different groups and entities, including on youth, the elderly, women and men, people who are vulnerable, particular professions, small and medium-sized enterprises, and others.
- [People] Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory.

Criticism of the first OEWG outcome document

Although the final report by the first OEWG in 2021 highlights the participation of women in cyber policy-making spaces, and recognises the importance of overcoming the gender digital divide, "discussions on these issues and what states could do about them are nearly absent across the different sections of the report."[36] Moreover, we believe that it could have gone further and considered gender as key in the discussions on cyber threats. Together with other civil society organisations, APC continues engaging in this process and renewing our calls in this regard.

35. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
36. Ferrari, V. (2021). Why should gender matter (more) for the OEWG? *Cyber Peace & Security Monitor, 1*(10). https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.10.pdf



APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS