UNIDIR STIMSON

COMPENDIUM

Mainstreaming Gender in Cybersecurity: A Compendium of Good Practices

ALLISON PYTLAK · DOMINIQUE STEINBRECHER · JESSICA ESPINOSA AZCARRAGA · KATHLEEN SCOGGIN · SHIMONA MOHAN

ACKNOWLEDGEMENTS

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. The work on this Compendium was funded by Global Affairs Canada.

The authors would like to thank the reviewers of this Compendium for their thoughtful comments, insights and feedback to improve the text, in particular Lisa Sharland (Stimson Center), Vanessa Murphy (ICRC), Tilman Rodenhäuser (ICRC), Renata Hessmann Dalaqua (UNIDIR) and Giacomo Persi Paoli (UNIDIR).

ABOUT UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. It is based in Geneva and assists the international community in developing the practical, innovative ideas needed to find solutions to critical security problems.

ABOUT THE STIMSON CENTER

The Stimson Center is a research institute based in Washington, D.C. The Stimson Center promotes international security and shared prosperity through applied research and independent analysis, global engagement, and policy innovation. Its Cyber Program focuses on tools and mechanisms that deter malicious cyber activity and address cyber harm through research, collaboration, and dialogue.

NOTE

The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessarily represent the views or opinions of the United Nations, UNIDIR, The Stimson Center, staff members or sponsors of either organization.

CITATION

Allison Pytlak, Dominique Steinbrecher, Jessica Espinosa Azcarraga, Kathleen Scoggin, Shimona Mohan (2026), "Mainstreaming Gender in Cybersecurity: A Compendium of Good Practices", UNIDIR, Geneva, doi.org/10.37559/SECTEC/26/CR/06.

Cover photo credit: Background image by Adobe Stock/kiattisak. Overlay image by Adobe Stock/Yuliya Kashirina. Design and layout by Trifecta Content Studio.

About the Authors

This report was produced by the UNIDIR Security and Technology Programme and the Stimson Center's Cyber Program.

Allison Pytlak, Dominique Steinbrecher, Jessica Espinosa Azcarraga, Kathleen Scoggin, and Shimona Mohan drafted the report; Andrea Gronke, Jiayue Lin, and Pavel Mraz contributed to the report.

Allison Pytlak

Senior Fellow and Director, Cyber Program, the Stimson Center

Allison Pytlak is Senior Fellow and Director of the Cyber Program at the Stimson Center. Her research on cybersecurity topics largely examines the interplay between cyber operations and international relations including multilateral governance structures such as United Nations processes and frameworks. Current projects focus on accountability and deterrence in cyberspace, including in the Indo-Pacific; multilateral cyber policymaking; and cybercrime scam operations. Prior to joining the Stimson Center, Pytlak managed the Disarmament Program of the Women's International League for Peace and Freedom and served in the Secretariat of the Control Arms Coalition. She has leveraged her significant experience in multilateral arms control and disarmament policy to identify opportunities for effectively advancing international law, norms and governance frameworks towards reducing cyber harm. Pytlak has also researched and published extensively about the gendered and human rights-based dimensions of digital security. She holds an Honours B.A. from the University of Toronto and an M.A. from the City University of New York.

Dominique Steinbrecher

Researcher, Security and Technology Programme, UNIDIR

Dominique Steinbrecher is a Researcher with UNIDIR's Security and Technology Programme, working on cybersecurity with a particular focus on international law. Her areas of expertise include international law, international humanitarian law and human rights, international security, and disarmament issues. Prior to joining UNIDIR, Dominique worked at the International Committee of the Red Cross in Geneva, the Cooperative Cyber Defence Centre of Excellence, the Non-Proliferation for Global Security Foundation, and the Civil Association for Equality and Justice. She holds an LL.M. from the Geneva Academy of International Humanitarian Law and Human Rights, a postgraduate degree in Security, Disarmament and Non-Proliferation, and a Law Degree from the University of Buenos Aires.

Jessica Espinosa Azcarraga

Digital Tools Coordinator, Security and Technology Programme, UNIDIR

Jessica Espinosa Azcarraga is a Programme Assistant with UNIDIR's Security and Technology Programme, where she provides operational, logistical, and content development support, contributing to capacity-building and research projects at the intersection of international security and emerging technologies. She holds a master's degree in Development Studies from the Geneva Graduate Institute and a bachelor's degree in International Relations from Anáhuac University in Mexico. Before joining UNIDIR, Jessica was Project Coordinator at the Swiss Digital Initiative and worked on projects funded by the United States Agency for International Development in Mexico. Her professional expertise spans topics such as gender, human rights, digital transformation, international cooperation, and project coordination.

Kathleen Scoggin

Research Assistant, Cyber Program, the Stimson Center

Kathleen Scoggin is a Research Assistant with the Stimson Center's Cyber Program. Her professional and academic work has covered topics such as the management of the global domain name system, the rise of autonomous weapons systems, data privacy, and the spyware market. Kathleen is an elected North American delegate to the At-Large Advisory Committee at the Internet Corporation for Assigned Names and Numbers. She is a former Youth Ambassador with the Internet Society, Fellow with the American Registry for Internet Numbers, and Junior Fellow working with the International Telecommunication Union. Kathleen holds a B.A. in International Studies and a minor in French from American University.

Shimona Mohan

Associate Researcher, Integrated Approaches - Gender & Disarmament and Security & Technology Programmes, UNIDIR

Shimona Mohan is an Associate Researcher with the Integrated Approaches - Gender & Disarmament and Security & Technology Programmes at UNIDIR. She is also one of the 100 Brilliant Women in AI Ethics for 2024. Her areas of focus include the intersections of security, emerging technologies (in particular AI and cybersecurity), gender and disarmament. Shimona has published and presented her research at various platforms, including intergovernmental, academic, civil society and track 1.5 forums. She also spearheads capacity-building programmes on AI and cybersecurity for government representatives and the stakeholder community working around emerging technology, including the UNIDIR Women in AI Fellowship. Shimona's previous work includes stints at the Observer Research Foundation, the Think20 Secretariat under India's G20 presidency in 2023, and the Carnegie Endowment for International Peace. She holds a master's degree in International Affairs from the Geneva Graduate Institute, a bachelor's degree (with honours) in Political Science from Miranda House at the University of Delhi, and certifications in Technology Law and Policy as well as Armament and Disarmament from India and Sweden respectively.

Abbreviations

AI	Artificial intelligence
CCB	Cyber capacity-building
CEDAW	Convention on the Elimination of All Forms of Discrimination against Women
ICRC	International Committee of the Red Cross
ICT	Information and communication technologies
ITU	International Telecommunication Union
NAP	National Action Plan
NCSS	National cybersecurity strategy
TFGBV	Technology-facilitated gender-based violence
UN Women	United Nations Entity for Gender Equality and the Empowerment of Women
WPS Agenda	Women, Peace and Security agenda

Table of Contents

Introduction

While the use of information and communication technologies (ICT) in the context of international security can have positive impacts,[1] it can simultaneously pose a significant risk to the safety and well-being of individuals.[2] With the expansion and increased complexity of cyberspace and the digital ecosystem, ICT threats can disproportionately affect different population groups, including on the basis of gender.[3]

Women, girls, men, boys and gender-diverse individuals are often impacted differently by cyber incidents. It has been recognized that digital violence on the basis of gender is one of the fastest-growing forms of online abuse, emphasizing the central role digital security and safety play in achieving gender equality.[4] Women and girls are disproportionately targeted by online harassment, privacy violations, and other forms of technology-facilitated violence, while being more exposed to the effects of data breaches and Internet shutdowns.[5] Men, and especially young men and boys, have more often been victims of online radicalization[6] and violent extremism.[7]

Similarly, women and girls are also more likely to encounter barriers to access, representation, and meaningful participation within the cybersecurity domain.[8] The lack of diversity in the field of cybersecurity and associated workforces constitutes a challenge to mainstreaming gender considerations at institutional levels.

Multilateral processes on State use of ICT have acknowledged the importance of narrowing the gender digital divide, promoting the full, equal, and meaningful participation of women in international ICT security decision-making, and integrating gender perspectives into cybersecurity policies and practices and capacity-building efforts.[9] This emphasizes the need for a comprehensive, inclusive, human-centred, and gender-responsive approach to cybersecurity that addresses differentiated and intersectional needs while embedding gender equality into policy, capacity-building, and cyberthreats-response frameworks. While research, policy initiatives, and capacity-building efforts on gender and cybersecurity have expanded in recent years, these developments have not yet been comprehensively mapped or systematically analysed.

---

1 Michelle Bachelet, "Human Rights in the Digital Age", UNOCHR, https://www.ohchr.org/en/speeches/2019/10/human-rights-digital-age.

2 General Assembly, Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, https://digitallibrary.un.org/record/3934214/files/A_76_135-EN.pdf?ln=en, para. 8.

3 General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, A/78/265, 1 August 2023, https://digitallibrary.un.org/nanna/record/4020967/files/A_78_265-EN.pdf?withWatermark=0&withMetadata=0&registerDownload=1&version=1https://digitallibrary.un.org/nanna/record/4020967/files/A_78_265-EN.pdf.

4 UN Woman, "UNITE To End Violence Against Women Campaign", https://www.unwomen.org/en/what-we-do/ending-violence-against-women/unite/theme.

5 Lisa Sharland et al., "System Update: Towards a Women, Peace and Cybersecurity Agenda", UNIDIR, 2021, https://doi.org/10.37559/GEN/2021/03.

6 Ana Carmo, "Why is the Manosphere on the Rise? UN Women Sounds the Alarm over Online Misogyny", 21 June 2025, UN News, https://news.un.org/en/story/2025/06/1164531.

7 Katrine Fangen and Inger Skjelsbæk, "The Role of Gender in Violent Extremism", in Milan Obaidi and Jonas Kunst (eds.), The Cambridge Handbook of the Psychology of Violent Extremism, 2025, https://www.cambridge.org/core/books/abs/cambridge-handbook-of-the-psychology-of-violent-extremism/role-of-gender-in-violent-extremism/5DF5ECE0813891009C2CB51B364FD6DC.

8 Katharine Millar and Verónica Ferrari, "A Novel Approach to the 11 UN Norms for Responsible State Behaviour in Cyberspace: Guidelines for Gendered Implementation", UNIDIR, 2025, https://unidir.org/wp-content/uploads/2025/05/UNIDIR_Novel_Approach_11_UN_Norms_Responsible_State_Behaviour_Cyberspace_Guidelines_Gendered_Implementation.pdf.

9 General Assembly, Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, para. 36; See also, General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, A/80/257, 24 July 2025.

Against this backdrop, in 2025, UNIDIR and the Stimson Center convened a series of multi-stakeholder workshops to identify practical ways in which gender can be mainstreamed into cybersecurity policies and practices. The workshops brought together a group of leading experts and practitioners from diverse communities of practice addressing critical areas of integrating gender considerations into cybersecurity. The resulting publication titled **Mainstreaming Gender in Cybersecurity: A Compendium of Good Practices** identifies relevant initiatives and good practices developed by Member States and the multistakeholder community and distils key insights, lessons learned, and recommendations on integrating gender perspectives into cybersecurity. The Compendium is intended to support Member States and other relevant stakeholders in their efforts to meaningfully integrate gender considerations in national ICT architectures and advance the implementation of the framework for responsible State behaviour in cyberspace[10] with a gender perspective in mind.

The Compendium addresses gender mainstreaming into cybersecurity through a substantive lens and a participatory lens. The substantive lens focuses on the specific impacts of ICT threats on different populations, including women, men, girls, boys and gender-diverse individuals, and how these experiences reveal systemic inequalities transposed into the digital realm. The participatory lens looks into the considerations around who shapes, implements, and leads cybersecurity policies and practices. The Compendium is structured into four chapters following the four focus areas of the workshops convened:

1. **Gendered threats and impacts of ICT** — Analyses how the use and misuse of ICT affects individuals and communities differently and illustrates the diversity of gendered impacts.
2. **Gender and International Law in Cyberspace** — Compiles examples and existing guidelines in which international law obligations and normative commitments can be interpreted and implemented in ways that reflect the lived experiences of those affected by ICT-related threats.
3. **Mainstreaming gender into national cyber policies and practices** — Examines gender equality commitments, multi-stakeholder participation, inclusive workforce development, and gender-responsive institutional mandates and incident reporting mechanisms guiding national cybersecurity and digital policies and practices.
4. **Gender-responsive cyber capacity-building** — Explores examples of targeted upskilling initiatives that can contribute to the full, equal, and meaningful participation and leadership of women and other marginalized groups in technology design and development, cybersecurity measures and incident response, in the formulation of policies, and in cybersecurity governance and diplomacy.

Each chapter summarizes workshop discussions, highlights insights and examples shared by participants, and includes a consolidated list of actionable recommendations intended to support the translation of analysis into practice. In line with this approach, these recommendations are presented as forward-looking considerations rather than prescriptive guidance, and are derived from practitioner-informed perspectives, good practices, and lessons learned.

10 UNIDIR, "Background to UN Discussions on Responsible State Behaviour", https://nationalcybersurvey.cyberpolicyportal.org/background-to-un-discussions-on-responsible-state-behaviour/

The Compendium offers concluding remarks reflecting on how integrating gender considerations into cybersecurity frameworks enables more comprehensive threats assessment, strengthens inclusive governance, and supports sustainable, long-term capacity-building and awareness. It also includes a list of cross-cutting recommendations stemming from the analyses in the chapters and overarching considerations gathered through the research project. Finally, a curated list of useful resources shared during workshop discussions or contributed by participants in follow-up exchanges is also included as a Toolbox of Resources at the end of the Compendium to guide further reading and engagement.

Methodology

This Compendium was developed using a combination of expert inputs from multi-stakeholder workshops organized by UNIDIR and the Stimson Center, written surveys of practitioners, and a supplementary review of literature. This combined research approach was purposefully chosen to connect academic research with practical perspectives and experiences. The project's goal was to gather relevant and practically applicable good practices and suggestions, while acknowledging that the most significant insights come directly from lived experiences and empirical evidence.[11]

UNIDIR and the Stimson Center co-hosted five virtual workshops during September and October 2025. These brought together a group of leading experts and practitioners from different communities of practice relevant to each topic and addressed the following themes:

1. International Law, Norms and Commitments in Cyberspace in the Context of Gender;
2. Mainstreaming Gender into National Cyber Policies and Practices;
3. Gender-Responsive Cyber Capacity Building; and
4. Threats and Impacts of ICT on Gender.

The workshops were structured to encourage open dialogue and included introductory presentations by selected experts to frame and contextualize the themes, followed by a discussion with targeted guiding questions. Discussions followed a semi-structured format, including general opening and closing questions to broadly highlight successful approaches to mainstreaming gender in cybersecurity based on their area of practice. Through this, several key approaches consistently stood out: funding, capacity-building, mentorship, training, representation, and data. The concepts revealed are the foundational pillars for the detailed good practices and key recommendations further developed in the following sections. Moreover, engagement among participants was guided through a dedicated list of questions on the specific topics of the workshop (see Annex I).

The workshops were conducted as closed-door sessions under the Chatham House rule to ensure open and free exchange. Therefore, comments and contributions included in this Compendium are not attributed unless explicitly consented to by individual participants. An anonymized online survey with guiding questions from the workshop was shared with participants and a broader group of stakeholders after each event to collect additional insights.[12]

UNIDIR and the Stimson Center prioritized diversity in regional and multi-stakeholder participation. In total, 89 practitioners took part in the discussions representing all five United Nations regional groups,[13] and featured kick-off presentations from various stakeholders:

11 The project was formally announced in December 2024 at the Internet Governance Forum in Saudi Arabia, during an Open Forum event titled "From Policy to Practice: Gender, Diversity and Cybersecurity". In July 2025, the Compendium drafting process was initiated through an interactive and informal closed-door session titled "Mainstreaming Gender in the New Permanent Mechanism on ICT Security and Diplomatic Processes", held during the July 2025 edition of the Women in International Security and Cyberspace Fellowship.

12 Eleven responses were received to the surveys across the different topics.

13 See United Nations, "Regional Groups of Member States", https://www.un.org/dgacm/en/content/regional-groups.

- representatives from the governments of Canada, Chile, Malawi, and the Netherlands;
- the United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), Asia and the Pacific;
- the Office of the United Nations High Commissioner for Human Rights (OHCHR);
- the International Committee of the Red Cross (ICRC);
- the Organization of American States;
- Fundación Karisma, a civil society organization based in Colombia; and
- independent subject matter experts.

The Compendium was drafted through a synthesis process that combined insights generated across the workshops, surveys, and follow-up inputs, with supplementary evidence from the literature review. Rather than reflecting the positions of the authors or specific institutions, the findings were distilled from recurring themes, areas of convergence, and illustrative good practices raised by participants across different communities of practice.

While this Compendium focuses on a gender perspective, it also acknowledges that gender does not shape peoples' experiences in isolation. Rather, it intersects with other overlapping factors, such as race, religion, ethnicity, age, disability, and class. In fact, as described by UN Women, the notion of 'gender' and gender attributes and relationships are socially constructed and learned through socialization processes.[14]

The Compendium also builds on existing relevant frameworks, such as the framework for responsible State behaviour in cyberspace developed through successive multilateral processes on ICT security in the General Assembly First Committee,[15] as well as the Women, Peace and Security Agenda (WPS), launched through the landmark Security Council resolution 1325 in 2000.[16]

14 UN Women, "Handbook on Gender Mainstreaming for Gender Equality Results", https://www.unwomen.org/sites/default/files/2022-02/Handbook-on-gender-mainstreaming-for-gender-equality-results-en.pdf.

15 See , General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, A/80/257, 24 July 2025.

16 See Department of Political and Peacebuilding Affairs, "Gender, Women, Peace and Security", https://dppa.un.org/en/women-peace-and-security.

1. Gendered Threats and Impacts of ICT

1.1. Introduction

The gendered impact of cyber operations and malicious use of ICT is an area of growing research and interest, yet one that remains poorly understood, under-documented, and not yet fully addressed by government policymakers or the technology industry. This chapter opens by illustrating the diversity of gendered impacts from cyber operations, identifies initiatives that have been effective in addressing gender-differentiated and gender-based cyberthreats, while also commenting on gaps and areas for improvement, including through recommendations.

Online spaces often mirror offline inequalities, with existing power structures, stereotypes, and social norms shaping people's safety, access, and participation online.[17] As one workshop participant noted, online and offline gender-based harms are interconnected and mutually reinforcing. Gender roles, stereotypes, and dynamics within any given society shape and influence online behaviour — including access to digital services and platforms.[18] Therefore, cyber incidents can impact people differently based on gender, age, and other characteristics. Gender should always be considered alongside other identifying characteristics such as race, religion, ethnicity, sexual orientation, and disability.

One of the prevalent observations was that women and gender minorities tend to be disproportionately impacted by technology-facilitated gender-based violence (TFGBV),[19] such as online harassment, doxxing, stalking, as well as the non-consensual sharing of intimate images. Practitioners highlighted that TFGBV relies on many of the same vectors studied in cybersecurity, like malware, phishing, and identity theft. Such violence can also take specific forms in complex contexts, such as situations of armed conflict.[20]

Gendered online disinformation campaigns against women or gender minorities active in public life were also referenced as a growing area of concern.[21] As just one example of gendered disinformation online, numerous national elections in 2024 demonstrated the growing scale of gendered disinformation efforts, including the use of artificial intelligence (AI)-generated deepfakes and bot networks to discourage women's political participation and leadership. Such campaigns not only undermine gender equality by

17 The Center for Feminist Foreign Policy, "Feminist Perspectives on the Militarisation of Cyberspace", 21 June 2023, https://centreforfeministforeignpolicy.org/2023/06/21/feminist-perspectives-on-the-militarisation-of-cyberspace/.

18 Deborah Brown and Allison Pytlak, "Why Gender Matters in International Cyber Security", April 2020, https://reachingcriticalwill.org/images/documents/Publications/gender-cybersecurity.pdf.

19 United Nations Population Fund, "Technology-facilitated Gender-based Violence: A Growing Threat", https://www.unfpa.org/TFGBV.

20 See UN Action against Sexual Violence in Conflict, "CRSV & Technology Facilitated GBV", December 2024, https://www.stoprapenow.org/resource/crsv-in-the-digital-sphere-december-2024/.

21 Ana Blatnik, "An Overlooked Threat To Democracy? Gendered Disinformation About Female Politicians", https://wiisglobal.org/an-overlooked-threat-to-democracy-gendered-disinformation-about-female-politicians/.

seeking to discredit women in public life but also pose broader national security risks by eroding trust in democratic processes and increasing social polarization.[22]

Some participants also noted that malicious cyber activities may have intended or unintended gendered impacts, such as those targeting infrastructure critical to the delivery of essential services. One expert highlighted the healthcare sector as frequently targeted by ransomware, hack-and-leak operations, distributed denial-of-service operations, and other malicious ICT activities.[23] When healthcare services are disrupted, sexual and reproductive healthcare, including maternity care, can be affected as well. Moreover, sexual and reproductive health providers may face particular risks because they handle highly sensitive medical and other personal data and provide services such as contraception, family planning, treatment of sexually transmitted diseases, and gender-affirming care which can be controversial in some societies and contexts.

Similarly, internet shutdowns were also frequently cited as illustrative of the link between societal gender roles and cyberharm. While Internet shutdowns affect entire communities, they have been shown to have distinct gendered impacts due to how people use and access the Internet which also often corresponds to one's gendered role in society. In some places women are restricted from owning devices or accessing public Internet spaces, for example; motivations for using digital technologies can also vary by gender. This situation can impact everything, from personal safety and well-being, to access to economic and educational opportunities.[24]

1.2. Key Observations

A key observation is that context matters. Gender and related mainstreaming efforts are, especially in multilateral settings, sometimes viewed as a western initiative, which can hinder mainstreaming efforts or practical implementation of gender-sensitive cybersecurity practices. Gender-sensitive approaches or frameworks may not always translate well across contexts and require adaptation. It was highlighted that sometimes threat actors deliberately target organizations advocating for gender equality or minority rights, through disinformation, defamation, or cyber operations against civil society online platforms. Discussion observed that a majority of the technology industry is based within and across a relatively small number of States of the, 'Global North' impacting the nature of relevant regulation, guidance, or protection frameworks in ways that may affect their contextual relevance or applicability elsewhere.

It was highlighted that digital or online systems can be inherently discriminatory. This can include the ways in which data is constructed and used, leading to gendered harms. Focusing solely on 'bad actors' may overlook the problematic ways in which data is constructed and used. One participant queried whether full government digitalization may lead to systems that prioritize infrastructure over people, while another

22 Stimson Center, "Gendered Disinformation: A National Security Threat?", https://www.stimson.org/event/gendered-disinformation-a-national-security-threat/.

23 Pavlina Pavlova, "Confronting Gendered Harm in Cyberspace is not a Matter of Social Justice — It's a National Security Imperative", 17 February 2025, https://www.justsecurity.org/107353/gendered-harm-cyberspace-not-social-justice-a-security-imperative/.

24 See UN Women, "When the Taliban Shut Down the Internet, Women Lost Their Lifeline to Aid, Learning, and Each Other", 10 October 2025, https://www.unwomen.org/en/news-stories/news/2025/10/when-the-taliban-shut-down-the-internet-women-lost-their-lifeline-to-aid-education-and-each-other; Deborah Brown and Allison Pytlak, "Why Gender Matters in International Cyber Security", April 2020, https://reachingcriticalwill.org/images/documents/Publications/gender-cybersecurity.pdf; and Access Now, "Why Internet Shutdowns are even Worse for Women", 17 March 2022, https://www.accessnow.org/internet-shutdowns-international-womens-day/.

observed that there is often a **"heteronormative approach to technology that lacks understanding of intersectional, vulnerabilities"** such as race, religion, ethnicity, sexual orientation, and disability as previously mentioned. Research in the Women, Peace and Security (WPS) domain around AI was cited to illustrate how automated decision-making systems, algorithmic bias, and surveillance tools may unintentionally reinforce gender inequality.[25] For example, a hiring algorithm trained on decades of male-dominated leadership data may systematically rank male candidates higher. Credit scoring and loan approval models can disadvantage women by weighting factors like career gaps or part-time work history, which disproportionately reflect gendered social expectations rather than actual creditworthiness. Text-generating language models trained on data primarily developed by men can replicate sexist language or gendered or discriminatory perspectives on a topic. For example, in national databases globally, only 50 per cent of indicators — such as those tracking education, health, and economic outcomes — have sex-disaggregated data, while 32 per cent lack any data from the past decade.[26]

Practitioners noted that vulnerabilities can stem both from technological weaknesses and from how ICT are designed, used, or managed. Yet threat actors are also becoming increasingly sophisticated and precise in their operations, making such risks difficult to mitigate — in the words of one workshop participant, **"it may not be possible to influence the bad actors."**

Low levels of awareness about data protection, privacy rights, and the vulnerabilities of older systems increase exposure to cyber risks. Conversely, when at-risk individuals increase their cyberhygiene, it can generate broader 'community demand' for stronger protections. As one participant noted, greater community understanding about privacy and security can compel developers to build in security systematically rather than as an afterthought.

It was emphasized that efforts to mainstream gender in cybersecurity threat prevention or mitigation cannot focus solely on women. While women are often disproportionately affected by TFGBV and other malicious uses of ICT, impacts can also affect men and gender minorities, and broader societal gender norms are a factor affecting technological access and use. For example, some men and boys face pressure to act as enforcers of traditional gender norms online, including expectations to monitor, control, or police the behavior of female partners, family members, or peers, or to protect them. Certain online spaces may also reinforce harmful forms of toxic masculinity by encouraging dominance, emotional suppression, and aggression while discouraging vulnerability; such echo-chamber environments are increasingly referred to as the 'manosphere'.[27] Some experts have found that extreme language used online often not only normalizes offline violence, usually against women and girls, but also is increasingly linked to radicalization and extremist ideologies.[28]

---

25 Genevieve Smith and Ishita Rustagi, "When Good Algorithms Go Sexist: Why and How to Advance AI Gender Equity", 31 March 2021, https://ssir.org/articles/entry/when_good_algorithms_go_sexist_why_and_how_to_advance_ai_gender_equity; see also for AI in the military domain, DCAF and Canadian Red Cross, "Operationalising IHL in AI Enabled and Autonomous Military Systems: Gender and WPS as Enablers of Lawful Use. Expert Roundtable Report", 9 March 2026, https://www.dcaf.ch/sites/default/files/imce/GSD/20260309OperationalisingIHL-AI_DCAF_CRC.pdf.

26 See, for example, Melanne Verveer and Jessica Anania, "The Risks of Gender-Blind Conflict Analysis", 20 March 2026, https://www.justsecurity.org/133898/gender-blind-conflict-analysis-risk/.

27 See, for example, UN Women, "What is the Manosphere and Why Should We Care?", 15 May 2025, https://www.unwomen.org/en/articles/explainer/what-is-the-manosphere-and-why-should-we-care.

28 Ibid.

More positively, ICT can and are being used to promote gender equality.[29] Social and messaging platforms are important forums for personal expression, political organizing, education, and community-building. Digital platforms enable women to access job markets, manage businesses, and earn income in ways that bypass existing barriers. Technology facilitates networking among activists and provides platforms for marginalized voices that might be excluded from traditional media.

1.3. Challenges and Gaps

Despite the fact that gendered dimensions of ICT threats and impacts is an area of growing research and interest, it is still one that remains under-documented and under-addressed at the policy level. Not all governments collect such data, creating national-level gaps and challenges in disseminating existing research and leveraging it to inform policy, law, and technology actors. While empirical research is incredibly valuable because of its ability to connect directly with affected groups, there is no sustained or regular resourcing to maintain such research.

Relatedly, the type of research and evidence required to demonstrate gendered impacts is complex and does not always translate neatly into arguments or evidence suitable for policy- or lawmakers. Further, this type of work also comes with risks for the researchers particularly in contexts of gender backlash, conflict, or areas of political fragility.

Moreover, not all monitoring and evaluation methodologies or formats account for gender. Specifically, concerns persist over evaluation metrics to track good practice in preventing and responding to gendered harms in cyberspace, in increasing gender diversity across cybersecurity-oriented professions more broadly, and in measuring the actual impact of policies, laws, and regulations which seek to reduce gendered harms online. For example, a 2024 study of multilateral cybersecurity forums sought to evaluate the link between improved levels of women's participation and the extent to which those forums produced gender-responsive policies or outcomes. While all of the surveyed forums did integrate gender considerations into their work, in some instances the tools or methods to assess implementation and impact of those outputs did not exist.[30]

Underpinning the above gaps and challenges, is a persistent gender digital divide relating to how genders access and use digital technologies, as well as gender diversity in the ICT sector, whether in policy, legal, or technical roles. According to the **International Telecommunication Union (ITU)**,[31] there were 189 million more men than women using the Internet globally in 2024. Moreover, women working in the private technology sector occupied less than one third of positions and faced a 21 per cent pay gap.[32] Women make up only an estimated 25 per cent of the cybersecurity workforce, creating representation gaps that can lead to overlooked gender-specific concerns in threat modelling, application design, datasets, and workplace policies.[33]

---

29 UN Women, Innovation for Gender Equality, 2019, https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/Library/Publications/2019/Innovation-for-gender-equality-en.pdfhttps://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/Library/Publications/2019/Innovation-for-gender-equality-en.pdf.

30 Allison Pytlak, "Gender and Cyber Diplomacy", in George Christou et al. (eds.), The Palgrave Handbook on Cyber Diplomacy, 2025, https://doi.org/10.1007/978-3-031-93385-1_7.

31 ITU, "The Gender Digital Divide", https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-the-gender-digital-divide/.

32 ITU, "Statement from ITU Secretary-General Doreen Bogdan-Martin on International Girls in ICT Day", 25 April 2024, https://www.itu.int/en/mediacentre/Pages/statement-2024-04-25-international-girls-in-ICT-Day.aspx.

33 Taken from Catalina Moreno's opening points; see ISC2, "Cybersecurity Workforce Study", https://www.isc2.org/Insights/2025/03/Women-Comprise-22-percent-of-the-Cybersecurity-Workforce.

These disparities are further shaped by intersecting factors such as age, race, language, and urban versus rural living conditions. As noted by one participant, women in the 'Global South' may face heightened impacts from cyber incidents and ICT misuse due to these overlapping challenges.

1.4. Good Practices, Lessons Learned, and Recommendations

A. Data Collection and Evidence-Based Policymaking

Participants highlighted that collecting data and evidence is an indispensable starting point for addressing gendered threats in cyberspace. Data can reveal which threats are most prevalent and who is most vulnerable in a specific context, and can help to inform the design of more effective policies and ensure diversity of the cybersecurity workforce.

Key Recommendations

- **Collect gender-disaggregated data and evidence** as an indispensable starting point for addressing gendered threats and impacts in cyberspace. Enhancing reporting and documentation of gendered cyberthreats helps to ensure systematic data collection to better understand gendered harms and recognize their scale and severity to inform the design of targeted remedies.
- **Promote data-gathering practices that respect confidentiality** and follow norms and standards for data privacy in regard to the individuals and communities they affect.
- **Disseminate and support dedicated research on gendered harms of malicious use of ICT, including by civil society working at local or national level**. At the workshops, a number of civil society organizations shared their research or initiatives that have captured specific gendered threats.
- These included case studies examining specific incidents, patterns, or types of threats, as well as quantitative data. Such research can supplement data collected by Member States, international organizations, and other entities, in order to inform policy and response.
- **Build clearer bridges between research on gendered threats and impacts and formulation of policy, law, and regulation** to achieve meaningful impact to reduce harms. This can include developing common repositories or databases for research, evidence, and information-sharing.

Good Practice: Data Collection, Gender Disaggregation, and Research

Several examples of good practice were shared by participants during the workshop, highlighting policies adopted by States and initiatives developed by non-State actors.

- Chile developed specific indicators to track implementation of **Sustainable Development Goal 5 on Gender Equality** and to help establish a baseline for data about women in technology roles in ways that link to broader efforts for poverty reduction.[34] This data-driven approach fostered greater policy coherence by presenting gender data in a neutral and technical manner, reducing the possibility of backlash and scepticism.
- **Global Affairs Canada** implements a **Gender-Based Analysis Plus (GBA Plus) tool** used to support the development of responsive and inclusive policies, programmes, and initiatives. Through the collection of indicators and data from internal and external sources, GBA Plus facilitates "understanding who is impacted by the issue or opportunity being addressed by the initiative; identifying how the initiative could be tailored to meet diverse needs of the people most impacted; and anticipating and mitigating any barriers to accessing or benefitting from the initiative".[35]
- A significant number of non-governmental organizations and academics have published research or are leading initiatives to better capture and highlight specific gendered impacts of cyber activity. These include the **Association for Progressive Communications**,[36] **Centre for Feminist Foreign Policy**,[37] **Karisma Foundation**,[38] **ICT4Peace**[39], **Women's International League for Peace and Freedom**
- **(WILPF)**,[40] and individual academics and researchers.[41] This research supplements data that is produced by international organizations such as the **ITU**,[42] **UN Women**,[43] and the **United Nations Office for Disarmament Affairs (UNODA)**.

34 See SDG Chile Hub, https://sdg-hub-chile-sdg.hub.arcgis.com/.

35 Government of Canada, "What is Gender-based Analysis Plus", https://www.canada.ca/en/women-gender-equality/gender-based-analysis-plus/what-gender-based-analysis-plus.html.

36 See Association for Progressive Communications, https://www.apc.org/en.

37 The Center for Feminist Foreign Policy, "Feminist Perspectives on the Militarisation of Cyberspace", 21 June 2023, https://centreforfeministforeignpolicy.org/2023/06/21/feminist-perspectives-on-the-militarisation-of-cyberspace/.

38 See Fundación Karisma, https://info.karisma.org.co/.

39 ICT4Peace, "Women's Peace and Security in the Digital Age: An emerging Agenda for Action", 28 October 2021, https://ict4peace.org/activities/womens-peace-and-security-in-the-digital-age-an-emerging-agenda-for-action.

40 Reaching Critical Will, "Information and Communications Technology (ICT) — Relevant WILPF Resources", https://reachingcriticalwill.org/disarmament-fora/ict#wilpf.

41 For example, Association for Progressive Communications, "Breaking Barriers: Examining the Digital Exclusion of Women and Online Gender-based Violence in Sudan", 18 November 2024, https://www.apc.org/en/pubs/breaking-barriers-examining-digital-exclusion-women-and-online-gender-based-violence-sudan; Anwar Mhajne and Alexis Henshaw, "Introduction", in Anwar Mhajne and Alexis Henshaw (eds.), Critical Perspectives on Cybersecurity: Feminist and Postcolonial Interventions, 2024, https://doi.org/10.1093/oso/9780197695883.003.0001; Anwar Mhajne, "Technology Facilitated Gender-based Violence in the Middle East", in Catherine Goetze and Khushi Singh Rathore (eds.), The Contemporary Reader of Feminist International Relations, 2025, https://www.taylorfrancis.com/chapters/edit/10.4324/9781003362012-37/technology-facilitated-gender-based-violence-middle-east-anwar-mhajne; Anwar Mhajne and Crystal Whetstone, "A Feminist Cybersecurity: Addressing the Crisis of Cyber(in)security", *International Affairs*, vol. 100, no. 6, 2024, https://doi.org/10.1093/ia/iiae234; Alexis Henshaw, "Norm Entrepreneurship and Gendered Cybersecurity: A View from Europe", *Global Studies Quarterly*, vol. 5, no. 3, https://doi.org/10.1093/isagsq/ksaf064; Anwar Mhajne , Leah Tabor, and Brian Traves, "Online Responses and Backlash to 'Women, Life, Freedom' Hashtag Activism", *Global Studies Quarterly*, vol. 5, no. 3, 2025, https://doi.org/10.1093/isagsq/ksaf063; Agnieszka Fal-Dutra Santos, "(Dis)connected? Women's Agency and Meaningful Participation in the Digital Space", *Peacebuilding*, vol. 14, 2026, https://doi.org/10.1080/21647259.2025.2583863.

42 ITU, "Gender Equality", https://www.itu.int/initiatives/gender-equality/.

43 See, for example, UN Women, "Cybersecurity Threats, Vulnerabilities and Resilience Among Women Human Rights Defenders and Civil Society in South-East Asia", 2024, https://asiapacific.unwomen.org/en/digital-library/publications/2024/05/cybersecurity-threats-vulnerabilities-and-resilience; see also UN Women, UN Women strategy: Preventing and eliminating technology-facilitated violence against women and girls, 2025, https://www.unwomen.org/en/digital-library/publications/2025/12/un-women-strategy-preventing-and-eliminating-technology-facilitated-violence-against-women-and-girls

B. Awareness-Raising and Upskilling

A recurring theme highlighted by participants concerned the importance of cyberhygiene, upskilling, and awareness-raising. The importance of early learning programmes, accessible information platforms, and 'digital hubs' in underprivileged areas that can offer training and access to ICT was emphasized. Relatedly, one participant noted that, **"Institutions also need to build internal capacity, not just hire gender consultants for specific projects. That means training cybersecurity teams to apply gender analysis in their day-to-day work and ensuring gender expertise is part of strategic decision-making"**.[44]

Key Recommendations

- **Strengthen cyber hygiene and awareness-raising** as a means to reduce gendered cyberthreats, as vulnerabilities can stem both from technological weaknesses and from how ICT are designed, used, and managed.
- **Develop early learning programmes, accessible information platforms, and digital hubs**, particularly in developing regions and targeting underserved communities to offer training in and access to ICT.
- Integrate learning about gendered threats and harm within cyber-related **capacity-building initiatives**.

C. Improving Diversity to Reduce Negative Gendered Impacts

Workshop participants highlighted that women should have equal opportunities to shape the policies and programmes that govern them. Greater inclusion may also contribute to more gender-responsive laws, policies, and technologies, helping to reduce gender-based harms. **"Without seeing women in those roles, you do not inspire the next generation"**, observed one participant.

Key Recommendations

- **Improve 'end to end' representation by ensuring that women are present across the entire cybersecurity talent pipeline**, from education and early career stages through to leadership, so that diverse perspectives can inform decisions, risk assessments, and solutions at every stage. Consider

44 Survey respondent for UNIDIR-Stimson Center workshops on gender mainstreaming in cybersecurity.

gender-sensitive approaches to both recruitment and retention practices (e.g. diverse interview panels, flex time, on-site childcare).

- **Build internal capacity on gender, rather than outsourcing relevant projects** or activities to specialized consultants. Train cybersecurity teams to apply gender analysis in their day-to-day work and ensure gender expertise is part of strategic decision-making.
- **Consider designations of 'critical infrastructure' with a gendered lens** by including services and facilities essential for people of all genders, gender identities and expressions, and sexual orientations.
- **Reduce the likelihood of inadvertent ICT misuse by building out diverse teams** in software and application development and testing, or assess the possible gender-based impacts of their misuse. Practitioners noted that vulnerabilities can stem both from technological weaknesses and from how ICT are designed, used, or managed.

2. Gender and International Law in Cyberspace

2.1. Introduction

This chapter identifies practical approaches to mainstreaming gender considerations into State commitments and legal obligations in cyberspace. International law is the set of rules and principles that govern the conduct and relations of subjects of the international community. It is a key pillar of the framework for responsible State behaviour since States agreed in 2013 that international law applies in cyberspace and is **"essential to maintaining peace and stability, and to promoting an open, secure, stable, accessible, and peaceful ICT environment"**.[45]

As highlighted in the previous chapter, ICT activities can result in direct and indirect harm to individuals.[46] Cyberthreats, as well as the cybersecurity measures adopted to address them, may have adverse impacts on legal rights and obligations, such as restrictions to freedom of expression or association, unlawful interferences with privacy and the integrity of electoral processes, and loss of access to vital services.[47] These impacts can disproportionately affect different groups, including on the basis of genders.[48]

In this regard, participants highlighted that mainstreaming gender in the interpretation and application of international law in cyberspace can strengthen its ability to address gendered cyber harms. This not only could make a substantive contribution to international legal theory but could also strengthen the role of international law in the effective protection and promotion of international peace and stability in cyberspace, including through a people-centred approach to international security.[49]

While States have stressed the need for a gender perspective in addressing ICT threats and the specific risks faced by persons in vulnerable situations,[50] as well as the importance of narrowing the gender digital

45 General Assembly, Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, para. 69; General Assembly, Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, A/AC.290/2021/CRP.2, 10 March 2021, para. 34.

46 General Assembly, Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, para. 9; General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, A/79/214, 22 July 2024, para. 18. On the potential human costs of cyber operations, see Laurent Gisel and Lukasz Olejnik, "The Potential Human Cost of Cyber Operations", ICRC, May 2019, https://www.icrc.org/sites/default/files/document/file_list/the-potential-human-cost-of-cyber-operations.pdf; see also General Assembly, Internet Shutdowns: Trends, Causes, Legal Implications and Impacts on a Range of Human Rights — Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/50/55, 13 May 2022, para. 1; for analysis on calls from States in the First Committee see Barrie Sander, "Recommendation 13(e)", in Office for Disarmament Affairs, Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology, 2017, https://www.researchgate.net/publication/326180320_Recommendations_13_g_and_h_Michael_Berk_Voluntary_Non-Binding_Norms_for_Responsible_State_Behaviour_in_the_Use_of_Information_and_Communications_Technology_-_A_Commentary.

47 See, for example, Freedom Online Coalition, "Joint Statement of the Human Rights Impact of Cybersecurity Laws, Practices and Policies", February 2020, p. 5, https://freedomonlinecoalition.com/wp-content/uploads/2021/06/FOC-Joint-Statement-on-the-Human-Rights-Impact-of-Cybersecurity-Laws-Practices-and-Policies.pdf.

48 See Office for Disarmament Affairs, "UN Security Council Open Debate on Cyber Security: Maintaining International Peace and Security in Cyberspace", 29 June 2021, https://un.mfa.ee/wp-content/uploads/sites/57/2021/06/Nakamitsu-29-June.pdf.

49 Cf. General Assembly, A/77/CRP.1/Add.8, 3 July 2023, https://docs.un.org/en/A/77/CRP.1/ADD.8.

50 General Assembly, Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, A/AC.292/2025/CRP.1, para. 28.

divide,[51] practical aids for interpretation and to address gender in States' international commitments and legal obligations have not yet been fully developed. Participants stressed the importance of action-oriented guidance on concrete and evidence-based measures to integrate gender into cybersecurity governance.

2.2. Key Observations

Participants highlighted the importance of gender-responsive guidance for the interpretation of international legal obligations. During the workshop, existing resources and tools, relevant approaches and initiatives, and authoritative interpretative efforts were described as useful guidance for legal advisers, experts, and practitioners in their efforts to apply international commitments and legal frameworks in cyberspace. These include, for example:

- relevant resolutions of the Human Rights Council;
- interpretative work of human rights treaty bodies, such as the Committee on the Elimination of Discrimination against Women and the Human Rights Committee;
- the work of independent experts under special procedures of the Human Rights Council;
- resolutions of the Security Council and relevant reports of the Secretary-General on the WPS Agenda;
- expert research and studies conducted by relevant international organizations, legal scholars, and civil society organizations; and
- regional and national interpretations of the application of international law in cyberspace addressing gender dimensions.

Importantly, practitioners highlighted the framework for responsible State behaviour as a key starting point for the integration of gender perspectives. For example, international human rights law has been addressed in both the voluntary norms and international law pillars of the framework. In this regard, norm E provides that, in ensuring the secure use of ICT, States should guarantee full respect for human rights. This norm can serve as an entry point for inclusion of gender considerations in multilateral processes on international ICT security, as gender equality is part of human rights. Through the development of an "additional layer of understanding" to norm E, States first recognized that the "[o]bservance of this norm can also contribute to promoting non-discrimination and narrowing the digital divide, including with regard to gender".[52] States have also agreed that their human rights obligations apply online just as they do offline,[53] thereby committing themselves to respect and protect human rights and fundamental freedoms in cyberspace in accordance with their international legal obligations.

51 General Assembly, Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security, A/76/135, 14 July 2021, para. 36 on norm E regarding respect and protect human rights and fundamental freedoms, where States agreed that "Observance of this norm can also contribute to promoting non-discrimination and narrowing the digital divide, including with regard to gender".

52 Ibid.

53 Ibid. Building from the interpretation of the Human Rights Council, see General Assembly, The Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/RES/20/8, 16 July 2012, para. 1.

2.3. Challenges and Gaps

Although participants stressed several initiatives and efforts to integrate a gender perspective in the application of international law in cyberspace, significant implementation gaps driven by structural, conceptual, and practical limitations were also identified.

Participants stressed that TFGBV continues to be insufficiently addressed within international legal frameworks, often being treated as less severe than physical violence despite its pervasive and harmful consequences.

Participants noted a persistent imbalance in cybersecurity discussions, where traditional international security considerations are often prioritized over the broader societal and individual impacts of malicious cyberactivity. As a result, cybersecurity measures focused on national security interests may lead to unlawful interferences with fundamental rights, with disproportionate effects on the basis of gender. This may also have an impact in legal interpretations that prioritize State-centric and narrow national security approaches to essential notions of international law, failing to account for gendered impacts in legal analysis and decision-making.

Such imbalances may be compounded by the lack of clear coordination and the potential resulting fragmentation among communities of practice — such as cybersecurity practitioners and experts, human rights and gender experts — whose various mandates and expertise sometimes hinder coherent and intersectional approaches.

2.4. Good Practices, Lessons Learned, and Recommendations

This section highlights different approaches to the interpretation of key branches of international law with a gender perspective. It presents four clusters of good practices and recommendations, stemming from concrete examples shared by participants on the following themes:

- a human-rights-based approach to cybersecurity;
- integrating gender in other branches of international law beyond human rights;
- reflecting gender in national and regional positions on how international law applies to cyberspace; and bridging gender gaps in communities of practice.

Each of the following subsections includes specific examples (within textboxes) of gender-sensitive interpretation and implementation of law that can guide legal advisers, experts, and practitioners in their application of international legal frameworks in cyberspace.

A. Human-Rights-Based Approach to Cybersecurity

The link between cybersecurity and human rights was emphasized by many participants, highlighting that individual security should be a core purpose of cybersecurity since cybersecurity and human rights

are complementary.[54] Numerous documents were cited to substantiate the interdependence between international peace and security and human rights including gender equality,[55] and to encourage a people-centred approach to cybersecurity.[56]

Participants highlighted the relevance of international human rights law to gender mainstreaming in the application of international law in cyberspace. In particular, they stressed the importance of upholding existing human rights obligations related to gender equality and non-discrimination in digital contexts.[57] This includes integrating gender considerations into the interpretation and application of rights relevant to cyberspace, such as freedom of expression and opinion, and the right to privacy.

Online gender-based violence was a concern shared by many participants, who highlighted the need for a clear understanding and definition of what constitutes such forms violence, how it is addressed under international human rights law,[58] and what measures can be adopted to eradicate it.

Recalling international human rights law treaties and drawing on current interpretations of how these rights apply in the digital domain, participants highlighted the importance of mainstreaming gender in national implementation of States' human rights obligations. In this context, participants consistently stressed that States should take positive measures to protect and fulfil human rights that address gender-specific risks and harms. These measures can include legislative frameworks, reporting mechanisms, and effective and accessible remedies to challenge human rights violations.[59] Participants also stressed the need to train, educate, and raise awareness among national authorities, including law enforcement, the judiciary, and human rights institutions, in order to implement international human rights law with a gender perspective in mind.

Importantly, participants highlighted that all cybersecurity measures and frameworks, including those designed to address inequalities and online gender-based violence, must also respect and safeguard the enjoyment of other human rights such as the right to privacy and data protection, the freedom of expression, access to information, and sexual and reproductive health rights.[60] Participants recalled that all measures must comply with international human rights law standards, that is, respect the principles of legality, necessity, proportionality, and legitimate objectives.[61]

---

54 In this regard, some participants stressed the work of the Freedom Online Coalition and views shared in their submissions in multilateral processes on ICT security; see, for example, Freedom Online Coalition, "FOC Joint Statement on the Human Rights Impact of Cybersecurity Laws, Practices and Policies,", February 2020, https://freedomonlinecoalition.com/wp-content/uploads/2021/06/FOC-Joint-Statement-on-the-Human-Rights-Impact-of-Cybersecurity-Laws-Practices-and-Policies.pdf.

55 United Nations, "Pact of the Future, Global Digital Compact and Declaration on Future Generations, Summit of the Future Outcome Documents", September 2024, https://www.un.org/sites/un2.un.org/files/sotf-the-pact-for-the-future.pdf.

56 United Nations, "A New Agenda for Peace", July 2023, https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-new-agenda-for-peace-en.pdf.

57 Cf. article 2, Universal Declaration of Human Rights; article 26 International Covenant on Civil and Political Rights; article 2International Covenant on Economic, Social and Cultural Rights; the Committee on Economic, Social and Cultural Rights, for example, has recognized age, nationality, marital and family status, sexual orientation and gender identity, disability, health status and economic and social situation as protected grounds; see Committee on Economic, Social and Cultural Rights, general comment No. 20, 2009, para. 13; specifically, the Convention on the Elimination of All Forms of Discrimination Against Women.

58 See, for example, General Assembly, Promotion and Protection of the Right to Freedom of Opinion and Expression, A/76/258, 30 July 2021, paras. 103, 104.

59 See, for example, General Assembly, Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/35/9, 5 May 2017, paras. 14, 38, and 60.

60 General Assembly, 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, A/HRC/38/47, para. 20; see also General Assembly, Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/35/9, 5 May 2017, para. 37.

61 For freedom of expression, see article 19(3) of the International Covenant on Civil and Political Rights; for the right to privacy, see article 17.

Key Recommendations

- **Put individual security at the centre of cybersecurity**, considering the complementarity and interdependence of human rights and international security.
- **Uphold human rights obligations on gender equality and non-discrimination** in the application of international human rights law in cyberspace, including on bridging the gender digital divide.
- **Address TFGBV as a subset of violence against women and girls** from a human security perspective, including the adoption of national legal, policy, and institutional frameworks that account for the specificities of harms and provide adequate measures to address and respond to TFGBV, including online gendered disinformation.
- **Advance the mainstreaming of gender considerations in the interpretation and application of all human rights obligations in cyberspace,** predominantly the right to freedom of expression and opinion and the right to privacy.
- **Ensure that all cybersecurity policies and measures are in accordance with international human rights law standards and obligations**, including having a legitimate aim, and respecting the principles of legality, necessity, and proportionality.
- **Consider the authoritative guidance and recommendation of relevant United Nations human rights bodies**, including on gender equality and non-discrimination, the right to be free from violence, the rights to freedom of expression and opinion, and the right to privacy.

Participants discussed various examples of authoritative interpretations and recommendations provided by relevant United Nations human rights bodies and experts. Some examples demonstrated how different treatment of offline gender-based violence versus online or technology-facilitated violence can result in inconsistent approaches and responses from authorities.

For instance, on bridging the gender digital divide, including disparities in the access to and the use of ICT, participants pointed to existing guidance provided by the **Human Rights Council**. The Council has stressed that "[i]nternational human rights norms and principles, especially equality, non-discrimination, inclusion, participation and the provision of effective remedies, should guide any action taken in response to issues of access, use and misuse of ICTs".[62] The Council has also identified factors influencing, preventing, and inhibiting women's access and use of ICT, including education, capacity and skills development, as well as sociocultural barriers and discriminatory legislation and policies, and ways to address them.[63]

With regard to the right to be free from violence and the prohibition of gender-based violence as a principle of international human rights law,[64] participants cited authoritative interpretations calling on States to

62 General Assembly, Promotion, Protection and Enjoyment of Human Rights on the Internet, A/HRC/35/9, 5 May 2017, para. 44.

63 Ibid., para. 11.

64 Committee on the Elimination of Discrimination against Women, General Recommendation No. 35 (updating No. 19), CEDAW/C/GC/35, 26 July 2017. For the legal basis in which this right is rooted, see the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW); see also, at the

address online and technology-facilitated gender-based violence as "part of the continuum of multiple, recurring and interrelated forms" of violence against women.[65] Participants also pointed to concrete international instruments, such as the **African Union Convention on Ending Violence Against Women and Girls**, which explicitly affirm that violence against women and girls includes online and cyber-enabled forms of violence.[66]

The **Convention on the Elimination of All Forms of Discrimination against Women** (CEDAW) was identified as a key source that addresses gender-based violence as a form of discrimination and a human rights violation. The Convention's application to online gender-based violence has been assessed specifically by its treaty body in its General Recommendation No. 35.

In Focus: The CEDAW and General Recommendation No. 35 on Gender-Based Violence against Women

The Committee on the Elimination of Discrimination against Women, the treaty body that monitors the implementation of the CEDAW, has explicitly referred to the digital dimension of violence against women in its General Recommendation No. 35, clarifying that gender-based violence includes technology-mediated violence. The recommendations of the Committee should guide States in the implementation of their obligations under the Convention.

The Committee has stressed that "gender-based violence against women ... manifests itself on a continuum of multiple, interrelated and recurring forms, in a range of settings, from private to public, including technology-mediated settings and in the contemporary globalized world it transcends national boundaries"[67] and that it "occurs in all spaces and spheres of human interaction, whether public or private" stressing "the redefinition of public and private through technology-mediated environments, such as contemporary forms of violence occurring online and in other digital environments".[68]

Apart from the general recommendations pertaining to all forms of violence,[69] the Committee has issued specific recommendations to encourage non-State actors, such as media organizations, to address gender-based violence that takes place through their services and platforms.[70]

regional level, the Inter-American Convention on the Prevention, Punishment and Eradication of Violence Against Women, the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence, the African Union Convention on Ending Violence Against Women and Girls, and the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa.

65 General Assembly, 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, A/HRC/38/47, 18 June 2018, para. 14.

66 See article 3(a) of the African Union Convention on Ending Violence Against Women and Girls.

67 Committee on the Elimination of Discrimination against Women, General Recommendation No. 35 (updating No. 19), CEDAW/C/GC/35, 26 July 2017, para. 6 (emphasis added).

68 Ibid., para. 20.

69 Ibid., paras. 27ff.

70 Ibid., para. 30(d).

While the general recommendation does not give a concrete definition of online gender-based violence, the work of human rights **Special Procedures** can provide guidance on specific behaviours that could be included in such a definition. For example, one participant cited the work of the **Special Rapporteur on violence against women**, referring to "online violence against women" as extending "to any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately".[71] Moreover, the **Special Rapporteur on the promotion and protection of freedom of opinion and expression** affirmed that "online gender-based violence" includes "both harmful speech and behaviour" and "is often sexist or misogynistic in nature and contains digital threats or incitement to physical or sexual violence".[72]

Furthermore, participants stressed that online gender-based violence can have a particular significance for the exercise of the rights to privacy and freedom of expression and opinion, since it can include harmful speech, including threats to physical or sexual violence, harassment, targeted unlawful surveillance, gendered censorship, and coercive discourses. Therefore, several interpretations advanced by human rights mechanisms were stressed as potentially relevant to mitigate these types of violations.

With regard to the right to privacy, participants highlighted the landmark Human Rights Council resolutions on the right to privacy in the digital age, which affirmed that "violations and abuses of the right to privacy in the digital age may affect all individuals, including with particular effects on women".[73] Participants discussed privacy risks addressed by the Council in this regard, including unduly used public surveillance to target specific communities on the basis of gender,[74] as well as threats against health or financial information, and knowledge about gender identities and sexual orientation.[75]

The work of the **Office of the United Nations High Commissioner for Human Rights** was also cited by participants, particularly its guidance on the key role of tools such as encryption to safeguard the exercise of rights, including the rights to privacy, freedom of opinion and expression, freedom of association and peaceful assembly, security, health and non-discrimination.[76] Other concerns highlighted by the **Special Rapporteur on the Right to Privacy** were presented by participants as relevant to be addressed through gender-sensitive interpretations of the law and mainstreaming gender into "the development and enforcement of privacy protection frameworks".[77] For example, a particular concern was the non-consensual sharing of health data, which has disproportionate effects on the basis of gender and can provide a strong disincentive to seeking care.[78]

71 General Assembly, 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, A/HRC/38/47, 18 June 2018, para. 23.

72 General Assembly, Promotion and Protection of the Right to Freedom of Opinion and Expression, A/76/258, 30 July 2021, para. 20 – the report also observes that "'Sextortion', doxing, trolling, online bullying and harassment, online stalking, online sexual harassment and the non-consensual sharing of intimate images have been identified as digitalized forms of violence against women by the Special Rapporteur on violence against women, its causes and consequences. Such acts can also involve smear campaigns, electronic sabotage, impersonation of the victim online and the sending of abusive messages in the victim's name".

73 General Assembly, The Right to Privacy in the Digital Age, A/HRC/RES/34/7, 7 April 2017.

74 General Assembly, The Right to Privacy in the Digital Age, A/HRC/51/17,4 August 2022, para. 50.

75 Ibid., para. 21.

76 Ibid.

77 General Assembly, Report of the Special Rapporteur on the Right to Privacy, A/HRC/40/63, 16 October 2019, para. 55.

78 Ibid., paras. 84–88.

With regard to the interpretation of the right to freedom of expression, participants highlighted guidance from United Nations human rights bodies on the implications of gendered online disinformation. In this context, resolutions of the **Human Rights Council** stressing that online disinformation campaigns can be used to deter women from participating in the public sphere, with certain groups of women, such as journalists, politicians, human rights defenders, and activists being disproportionately targeted, were cited as particularly relevant.[79] Additionally, participants referred to the work of the **Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression**. Specifically, they highlighted a report addressing gendered disinformation as a strategy to silence the free expression of women and gender-diverse individuals as a form of gender-based violence[80] with the potential to undermine the diversity of public debate,[81] inclusive democracy, and sustainable development.[82] Participants recalled the Special Rapporteur's guidance that measures to address online gender-based violence should not be used as a pretext by States for unlawful restrictions of other rights, such as freedom of expression, need to comply with all human rights law requirements,[83] and should be "strictly and narrowly construed".[84]

B. Integrate Gender in Other Branches of International Law

Beyond human rights law, participants stressed the importance of gender mainstreaming into other existing international law obligations by factoring the specific ICT-related forms of harm in the interpretation and implementation of different rules and principles of international law, including those enshrined in the **Charter of the United Nations**. They highlighted that, since gender inequalities are embedded in contexts where cyber operations between States occur and are a factor that influences the effects of such a threat, they should be addressed under international law applicable to such operations.[85] For example, in applying specific rules and principles in cyberspace, such as sovereignty, non-intervention, or the prohibition of the use of force, many States have highlighted the need to determine if the required threshold for a violation has been met on a case-by-case basis.[86] For that, some States have referred to the nature of the target as relevant to determine if the required threshold has been met in a specific case, such as cyber operations targeting critical infrastructure, or infrastructure key for the delivery of essential or public services. Therefore, participants stressed that how States define critical infrastructure can affect how gender and other minorities are protected from online harm under international law.

While internationally there is no agreed definition of critical infrastructure,[87] participants highlighted that States can support gender-sensitive approaches to defining critical infrastructure nationally in a manner that reflects diverse needs of all groups and recognizes that cyber operations targeting certain sectors may disproportionately impact certain groups, including on the basis of gender. An example shared by

79 General Assembly, Role of States in Countering the Negative Impact of Disinformation on the Enjoyment and Realization of Human Rights, A/HRC/RES/49/21, 30 March 2022; see also General Assembly, Promotion and Protection of the Right to Freedom of Opinion and Expression, A/76/258, 30 July 2021, para. 102.

80 General Assembly, Promotion and Protection of the Right to freedomFreedom of Opinion and Expression, A/78/288, 7 August 2023, para. 10.

81 General Assembly, Promotion and Protection of the Right to Freedom of Opinion and Expression, A/76/258, 30 July 2021, para. 102.

82 General Assembly, Promotion and Protection of the Right to Freedom of Opinion and Expression, A/78/288, 7 August 2023, para. 1, also paras. 13, 20. On the impact on political participation and democracy, see General Assembly, Freedom of Expression and Elections in the Digital Age, A/HRC/59/50, 11 June 2025.

83 General Assembly, Promotion and Protection of the Right to Freedom of Opinion and Expression, A/76/258, 30 July 2021, paras. 103, 104; see also General Assembly, Promotion and Protection of the Right to Freedom of Opinion and Expression, A/78/288, 7 August 2023, para. 117.

84 Ibid., para. 127.

85 See *mutatis mutandis*, ICRC, "Gendered Impacts of Armed Conflict: Exploring Implications for IHL Governing the Conduct of Hostilities", 2022, https://library.icrc.org/library/docs/DOC/icrc-4634-002.pdf, p. 11.

86 See national positions available at the UNIDIR Cyber Policy Portal, https://cyberpolicyportal.org/.

87 See General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, A/80/257, 2025, para. 17.

one participant stressed that **"research and education sectors are the least likely to be designated as critical infrastructure worldwide. At the same time, schools have seen a sharp increase in cyber incidents across regions when ransomware attacks caused prolonged disruptions. These attacks create [disproportionate] burdens for individuals with caregiving responsibilities and reduce workforce participation"**.[88]

In their national positions, many States identify coercive interference with another State's ability to hold an election as a potential form of prohibited intervention under international law.[89] As such, interference in elections may have a strong gender dimension, including through gendered online disinformation campaigns that aim to "mislead the public, create division and affect electoral outcomes" by disproportionately targeting women politicians.[90] Such campaigns impact both human rights and the rights of States,[91] since cyberthreats targeting elections may pose threats to national security, undermine democratic processes, and put individuals at risk.

Many participants noted that armed conflict impacts genders differently, for example due to systemic inequalities, a continuum of gender-based violence, underreported violations, and unequal access to information and essential services. Many practitioners stressed that the use of ICT in armed conflict may introduce new gendered risks and vulnerabilities, and therefore called for mainstreaming gender considerations into the interpretation and application of international humanitarian law in cyberspace.[92]

Among other relevant international humanitarian law obligations, discrimination in its application based on race, colour, sex, language, religion or belief, political or other opinion, national or social origin, wealth, birth or other status, or on any other similar criteria is prohibited;[93] sexual violence is also prohibited.[94] In this context, one participant noted that **"a gender perspective to the interpretation of [international humanitarian law] may support the aim of reaching common understandings on its application in cyberspace by answering some of the outstanding questions and divergent views and offer another layer of analysis outside the strictly national security approach, for example to definitions such as the notion of 'attack' or 'data', integrating harms or notions of violence that may be otherwise overlooked"**.[95] States have already recognized that women, men, girls, and boys can be affected differently by the use of ICT in armed conflict, and thus such differences need to be considered when implementing and applying international humanitarian law.[96]

88 Survey respondent for UNIDIR-Stimson Center workshops on gender mainstreaming in cybersecurity.

89 See the national positions of Australia, Austria, Brazil, Canada, Germany, Israel, New Zealand, Norway, Singapore, the United Kingdom, and the United States. All national and regional positions are available at the UNIDIR Cyber Policy Portal, https://cyberpolicyportal.org/.

90 Katharine Millar and Verónica Ferrari, "A Novel Approach to the 11 UN Norms for Responsible State Behaviour in Cyberspace: Guidelines for Gendered Implementation", UNIDIR, 2025, https://unidir.org/wp-content/uploads/2025/05/UNIDIR_Novel_Approach_11_UN_Norms_Responsible_State_Behaviour_Cyberspace_Guidelines_Gendered_Implementation.pdf, https://unidir.org/wp-content/uploads/2025/05/UNIDIR_Novel_Approach_11_UN_Norms_Responsible_State_Behaviour_Cyberspace_Guidelines_Gendered_Implementation.pdf, p. 26.

91 Ibid.

92 See, for example, ICRC, "Gendered Impacts of Armed Conflict: Exploring Implications for IHL Governing the Conduct of Hostilities", 2022, https://library.icrc.org/library/docs/DOC/icrc-4634-002.pdf, p. 11; this document was discussed extensively during the workshop.

93 See, for example, common article 3 to the Geneva Conventions; article 16, Third Geneva Convention; article 13, Fourth Geneva Convention; and article 75, Additional Protocol I. See also ICRC, Study on Customary IHL, Rule 88, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule88.

94 See, for example, article 75, Additional Protocol I; article 4, Additional Protocol II; article 27, Fourth Geneva Convention. See also, ICRC, Study on Customary IHL, Rule 93, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule93.

95 Participant in UNIDIR-Stimson Center workshops on gender mainstreaming in cybersecurity.

96 International Conference of the Red Cross and Red Crescent, Resolution 34IC/24/R2, Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict, October 2024.

Key Recommendations

- **Consider an intersectional approach to integrating gender considerations** in international law interpretation and implementation beyond human rights law.
- **Promote a gender-sensitive approach to the interpretation of key concepts** that may underpin the application of concrete rules and principles**,** such as the notion of 'inherent governmental functions', 'coercion', and the definition of 'critical infrastructure'.
- **Integrate gender perspectives in international humanitarian law** interpretation and operationalization in cyberspace, to account for and to mitigate gender-specific harms, and consider the gender dimensions of armed conflicts.

During the workshop, participants shared examples of studies that could guide research and development of relevant international law interpretations that account for gendered risks and vulnerabilities introduced by the State use of ICT.

With regard to international humanitarian law, participants highlighted that relevant stakeholders, such as the **International Committee of the Red Cross** (ICRC), have advanced empirical research into gender dimensions of armed conflicts[97] and the application of a gender perspective in the planning and conduct of military operations under international humanitarian law.[98] Participants noted that while not scoped expressly to cyberspace, insights from this body of knowledge may nevertheless provide an important foundation for developing gender-responsive interpretations of international humanitarian law in the online domain.

In Focus: Integrating Gender Perspectives into the Application of International Humanitarian Law in Cyberspace

Examples and suggestions shared by participants included:

- **Factor gender-specific harms in the notion of 'civilian harm'** when assessing cyber operations under international humanitarian law rules on the conduct of hostilities, such as the principles of distinction, proportionality, and precautions, to understand their humanitarian consequences.[99] As pointed out by the ICRC, "from a legal standpoint, incorporating a gender perspective can help ensure

97 ICRC, "Gendered Impacts of Armed Conflict: Exploring Implications for IHL Governing the Conduct of Hostilities", 2022, https://library.icrc.org/library/docs/DOC/icrc-4634-002.pdf.

98 ICRC, NCGM and Swedish Red Cross, "International Humanitarian Law and a Gender Perspective in the Planning and Conduct of Military Operations", 2024, https://www.rodakorset.se/contentassets/0df6788aa32243b08fea2b03afb5438c/international-humanitarian-law-and-a-gender-perspective-in-the-planning-and-conduct-of-military-operations.pdf.

99 See, for example, ICRC, "Gendered Impacts of Armed Conflict: Exploring Implications for IHL Governing the Conduct of Hostilities", 2022, https://library.icrc.org/library/docs/DOC/icrc-4634-002.pdf, pp. 7, 11–21.

better respect" for international humanitarian law[100] since the "[e]xpected civilian harm is more likely to be accurately assessed if it is considered from a gender perspective".[101]

- **Factor in specific harms caused by cyber operations targeting specific types of civilian objects**, such as hospitals providing gynecological and obstetric care, when evaluating reasonably foreseeable civilian harm, assessing the 'excessiveness' thereof,[102] and adopting specific precautionary measures. The latter could also be analysed through a gender lens, such as the gender digital divide in access to ICT when considering effective warnings.[103]
- Interpret certain international humanitarian law prohibitions, such as the prohibition of adverse distinction[104] and the prohibition of all forms of sexual violence,[105] to **consider the different forms of online gender-based violence during armed conflict**, for example, online distribution of images of victims of rape during armed conflict or using ICT to incite gender-based violence. The latter should be interpreted in relation to the prohibition of encouraging international humanitarian law violations.[106] Examples were shared of views put forward by some States in the realm of dedicated international humanitarian law initiatives on the risks and prevention of online sexual violence in armed conflict.[107]
- International humanitarian law addresses the **spread of harmful information** through ICT, such as threats of violence against civilians and other protected persons disseminated through ICTs. It should be considered that certain groups will be disproportionately affected on the basis of gender.
- Other suggestions mentioned the integration of a gender perspective to the **data protection of information pertaining to the restoration of family links**, including the processing of personal data of beneficiaries.[108] Moreover, and subject to the diverse interpretations that States have advanced in the matter, the **protection of specific data under international humanitarian law**, such as data pertaining to medical missions or humanitarian organizations, under the obligation to respect

100 ICRC, NCGM and Swedish Red Cross, "International Humanitarian Law and a Gender Perspective in the Planning and Conduct of Military Operations", 2024, https://www.rodakorset.se/contentassets/0df6788aa32243b08fea2b03afb5438c/international-humanitarian-law-and-a-gender-perspective-in-the-planning-and-conduct-of-military-operations.pdf, p. 17.

101 ICRC, "Gendered Impacts of Armed Conflict: Exploring Implications for IHL Governing the Conduct of Hostilities", 2022, https://library.icrc.org/library/docs/DOC/icrc-4634-002.pdf, p. 7.

102 See, for example, ICRC, "Gendered Impacts of Armed Conflict: Exploring Implications for IHL Governing the Conduct of Hostilities", 2022, https://library.icrc.org/library/docs/DOC/icrc-4634-002.pdf, p. 17. On the protection of hospitals against cyberoperations during armed conflict, see ICRC, "Protection of Medical Personnel, Units and Transports during Armed Conflict", 2025, https://www.icrc.org/sites/default/files/2025-02/06_Medical_facilities.pdf.

103 See, for example, ICRC, "Gendered Impacts of Armed Conflict: Exploring Implications for IHL Governing the Conduct of Hostilities", 2022 https://library.icrc.org/library/docs/DOC/icrc-4634-002.pdf, p. 18.

104 See ICRC, NCGM and Swedish Red Cross, "International Humanitarian Law and a Gender Perspective in the Planning and Conduct of Military Operations", 2024, https://www.rodakorset.se/contentassets/0df6788aa32243b08fea2b03afb5438c/international-humanitarian-law-and-a-gender-perspective-in-the-planning-and-conduct-of-military-operations.pdfhttps://www.rodakorset.se/contentassets/0df6788aa32243b08fea2b03afb5438c/international-humanitarian-law-and-a-gender-perspective-in-the-planning-and-conduct-of-military-operations.pdf, p. 22. See First Geneva Convention, art. 12(2); Second Geneva Convention, art. 12(2); Third Geneva Convnetion, art. 16; Fourth Geneva Convention, art. 27(3); Additional Protocol I to the Geneva Conventions, art. 75(1); Additional Protocol II to the Geneva Conventions, art. 4. See also Commentaries to all the Geneva Conventions and Additional Protocols, on the topic of 'gender', at https://ihl-databases.icrc.org/en/ihl-treaties/geneva-conventions-1949additional-protocols-and-their-commentaries.

105 Cf. Additional Protocol I to the Geneva Conventions, arts. 75 and 76; Additional Protocol II to the Geneva Conventions, art. 4; common article 3 to the Geneva Conventions.

106 Cf. common article 1 to the Geneva Conventions of 1949; see also resolution 33IC/19/R4, adopted at the 33rd International Conference of the Red Cross and Red Crescent, op. para. 4, https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL-_CLEAN_ADOPTED_en.pdf.

107 See Humanity in War, Draft outcome document for fourth consultation, Workstream 6 – Upholding International Humanitarian Law in the use of Information and Communication Technologies during Armed Conflicts, Co-Chaires by Ghana, Luxembourg, Mexico, Switzerland and the ICRC, 1 April 2026, https://www.upholdhumanityinwar.org/en/documentation?field_state_target_id=All&field_workstream_target_id=All&field_type_target_id=All&field_language_target_id=All&name=outcome#documentation.

108 For example, gender considerations could be mainstreaming into the Restoring Family Links Code of Conduct on Data Protection; see also resolution 33IC/19/R4, adopted at the 33rd International Conference of the Red Cross and Red Crescent, https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL-_CLEAN_ADOPTED_en.pdf.

and protect them under international humanitarian law,[109] could also be addressed from a gender perspective, including the protection of specific sensitive data, such as data pertaining to reproductive healthcare.

C. Gender in Regional and National Positions

Participants highlighted the importance of articulating national and regional positions on how international law applies in cyberspace, and how these positions can become relevant key avenues to integrate gender into national and regional views on international law,[110] particularly for States that have not yet issued or developed a national position, or are planning to update or complement it.[111]

Key Recommendations

- **Regional and national positions on how international law applies in cyberspace** are key to advancing national views on the interpretation of international law in its application to cyberspace. As done by some States, national positions could integrate gender in their legal interpretations.
- **Consider a cross-cutting integration of gender considerations** in regional or national views on international law, including but not limited to chapters on the application of international human rights law in cyberspace.

Participants also recalled that some national positions have included gender. The following box summarizes the various ways in which some Member States have integrated gender considerations in their views on how international law applies in cyberspace.

109 Cf. First Geneva Convention I, art. 19; Second Geneva Convention, art. 12; Fourth Geneva Convention, art. 18; Additional Protocol I to the Geneva Conventions, art. 12; Additional Protocol II to the Geneva Conventions, art. 11; see also ICRC, "Protection of Medical Personnel, Units and Transports during Armed Conflict, Cyber Operations during Armed Conflict", February 2025, https://www.icrc.org/sites/default/files/2025-02/06_Medical_facilities.pdf; ICRC, "Protection of Humanitarian Personnel and Objects during Armed Conflict", February 2025, https://www.icrc.org/sites/default/files/2025-02/05_Humanitarian-org.pdf.

110 To date, 37 individual Member States have developed and published their national positions on the application of international law to State use of ICT, alongside two regional positions of the African Union and European Union. See UNIDIR, Cyber Policy Portal, available at https://cyberpolicyportal.org/, accessed 27 May 2026.

111 Participant in UNIDIR-Stimson Center workshops on gender mainstreaming in cybersecurity.

Good Practices: Examples of Regional and National Positions on the Application of International Law in Cyberspace with Gender Considerations

Broader or indirect references in national and regional positions

- Some States have included general references to equality and non-discrimination in international human rights law chapters, such as those of **Australia, Canada, Costa Rica, Czech Republic, the Common African Position**, the and Common Declaration of the **European Union**, and of **Australia, Canada, Costa Rica, Czechia, the Republic of Korea,** and **Thailand**.[112]
- Some positions make specific references to women's protection and empowerment, such as those of the **Common African Position** and of the **Republic of Korea.**[113]
- Some national positions make references to specific sources that address gender-specific aspects of certain rights, such as the position of **Thailand**.[114]

Explicit references to gender in national positions

- **Costa Rica's** position[115] highlights the imperative of addressing the gendered impact of cyber operations, with particular references to groups of people that can be especially targeted by malicious uses of ICT. It also notes the inequality in ICT access and knowledge, including on the basis of gender. Moreover, the position addresses gender in both its international human rights law[116] and international humanitarian law sections.[117]
- **Colombia's** position[118] has also integrated gender considerations in its interpretations of the application of both international human rights law, including on addressing the gender digital divide,[119] and the application of international humanitarian law in cyberspace.[120]

---

112 For example, the positions of Australia, Canada, Thailand, and the Common African Position stress the need to guarantee human rights online without distinction and/or discrimination of any kind, while the positions of Canada, Costa Rica, the Czech Republic, the Republic of Korea, and the Common Declaration of the European Union, include specific references to freedom from discrimination and right to equality and non-discrimination. The national positions are available at UNIDIR Cyber Policy Portal Database, https://database.cyberpolicyportal.org/en/.

113 For example, the national position of the Republic of Korea stresses that fundamental rights must "be protected and upheld in cyberspace for all individuals, including women and socially vulnerable groups". The Common African Position stresses "the importance of bridging the digital divide to ensuring the full enjoyment of human rights. In this regard, States shall contribute to further empowering women and girls".

114 For example, Thailand's national position makes explicit reference to the Human Rights Council reports 53/29 (2023) and 54/21 (2023), both of which refer to gender-specific aspects of the right to privacy in the digital age, gender-based violence through or amplified by the use of technology, and gender equality and non-discrimination. See Human Rights Council, New and emerging digital technologies and human rights, A/HRC/RES/53/29, 14 July 2023; Human Rights Council, Right to privacy in the digital age, A/HRC/RES/54/21, 12 October 2023.

115 Ministry of Foreign Affairs of Costa Rica, "Costa Rica's Position on the Application of International Law in Cyberspace", 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf.

116 For example, the position acknowledges that women have been particularly affected by cyberoperations, including "electronic surveillance, hate speech, doxing, cyber bullying, and harassment" and invokes States' obligations regarding the rights of women online, with particular reference to the Convention on the Elimination of All Forms of Discrimination against Women.

117 For example, the position stresses the need to integrate a gender perspective into the planning and execution of information and psychological operations during armed conflict.

118 Ministry of Foreign Affairs of Colombia, "Colombia's National Position on the Application of International Law in Cyberspace", 2025, https://cms.cyberpolicyportal.org/uploads/Colombia_NP_Cyber_PDF_Ingles_1_d6c0afafdd.pdf.

119 For example, the position stresses the importance of recognizing the "unique challenges and vulnerabilities faced by women and other... marginalized groups online" and that mainstreaming a "gender-responsive perspective in all relevant efforts ensures that international legal frameworks are inclusive and equitable, safeguarding the rights of all individuals".

120 With regard to IHL, the position highlights the relevance of analysing under international humanitarian law specific impacts of cyber operations on people in vulnerable situations, including "*children, women, and the LGBTQ+ / SOGIESC community*".

- **Sweden's** position[121] refers to the need to close the gender digital divide in its international human rights law section.

D. Bridge Gender Gaps across Communities of Practice

Participants called for empowering women and gender-diverse professionals to meaningfully and consistently participate in the development and implementation of international law. Doing so would ensure that a broader range of perspectives are represented, thereby leading to more effective and gender-responsive implementation of legal and normative frameworks governing the State use of ICT.
A recurring point in the discussions was the importance of bridging gaps across communities of practice to ensure coherent international law approaches and rights-respecting cybersecurity measures, and to avoid overlap or duplication of efforts. This should include promoting sustained engagement and coordination among cybersecurity experts, human rights practitioners, and existing international mechanisms. The development of standards and interpretative approaches driven by human rights processes can inform the application of international law in cyberspace as well as encourage broader cybersecurity discussions to consider a human-centric perspective. In this regard, participants recalled that States have affirmed the need to engage external voices, including human rights experts, in policy-making processes relevant to international ICT security.[122]

Similarly, participants stressed the need to foster coherent approaches across gender and digital rights communities. One specific view warned that **"advocacy on one [issue] should not be to the detriment of the other"**. This would include ensuring that efforts to combat TFGBV do not inadvertently align with expansions of State information control and surveillance that may negatively impact other rights, such as the right to privacy.[123]

Finally, there was broad support to strengthen links between the **WPS Agenda**[124] and the application of international law in cyberspace to enhance the fulfilment of rights, such as equality, non-discrimination, and the prevention of and protection from online gender-based violence.[125]

121 Government Offices of Sweden, "Position Paper on the Application of International Law in Cyberspace", July 2022, https://www.government.se/contentassets/3c2cb6febd0e4ab0bd542f653283b140/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf.

122 See additional layer of understanding of norm E — General Assembly, Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135 (14 July 2021), paras. 36–41.

123 Survey respondent for UNIDIR-Stimson Center workshops on gender mainstreaming in cybersecurity.

124 As developed through the Security Council resolution 1325 and subsequent; see Department of Political and Peacebuilding Affairs, "Gender, Women, Peace and Security", https://dppa.un.org/en/women-peace-and-security.

125 See Lisa Sharland et al., "System Update: Towards a Women, Peace and Cybersecurity Agenda", UNIDIR, 2021, https://doi.org/10.37559/GEN/2021/03, pp. 23–25; see also United Nations, "Digital Breakthroughs Must Serve Betterment of People, Planet, Speakers Tell Security Council during Day-Long Debate on Evolving Cyberspace Threats", 20 June 2024, https://press.un.org/en/2024/sc15738.doc.htm.

Key Recommendations

- **Empower women and gender-diverse professionals** to meaningfully and consistently participate in all levels of cybersecurity governance, including policy development, legal interpretation and implementation, and decision-making.
- **Promote sustained, structured engagement and coordination** among cybersecurity experts and multilateral processes, human rights practitioners, and international mechanisms. Bridging gaps across communities working on different aspects of international law can ensure coherent approaches and rights-respecting cybersecurity measures.

3. Mainstreaming Gender in National Cyber Policies and Practices

3.1. Introduction

Integrating gender considerations in national cyber policies and practices is key to advancing equitable and effective cybersecurity frameworks that meaningfully address and resolve digital harms across different communities. At the same time, governance frameworks such as national action plans (NAPs) for the WPS Agenda, can incorporate cybersecurity considerations and consequently break down existing silos between policy areas.

National cybersecurity strategies (NCSS) are a key instrument through which governments organize and implement their commitments to digital security, national resilience, and the protections of citizens online.[126] Through them, States articulate their approaches to cybersecurity and define institutional responsibilities, coordination mechanisms, and measurable outcomes aligned with broader national security, governance, and development policies.[127] According to **ITU's 2024 Global Cybersecurity Index**,[128] more than 110 States have dedicated NCSS in place, reflecting the recognition that cybersecurity has become foundational to national security and stability.

NCSS are evolving beyond their original focus on infrastructure and threat mitigation[129] to function as frameworks that define how governments plan to respond to emerging risks and intend to address issues such as critical infrastructure protection, incident response, cybercrime, and capacity-building. Such strategies thus serve not only as plans for defensive readiness but also as frameworks through which governments set guidelines for achieving accountability, individual rights, and resilience in cyberspace. Therefore, NCSS constitute central instruments for shaping a secure, resilient, and inclusive digital space. Ultimately, mainstreaming gender into national cybersecurity policies and practices is a matter of strategic foresight, not symbolic inclusion. By embedding gender considerations into policy design and governance, States can craft more comprehensive, legitimate, and resilient responses to the challenges of the digital age.

Drawing from specific examples shared by State representatives during the workshop, this chapter considers the extent to which gender is currently being mainstreamed within national cybersecurity policies, notably NCSS and related work. It highlights practitioners' insights into how national strategies can incorporate more equitable, participatory, and socially aware approaches to cybersecurity. It identifies

126 ITU, "National Strategies", https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx.

127 Ibid.

128 ITU, "Global Cybersecurity Index 2024", https://www.itu.int/epublications/zh/publication/global-cybersecurity-index-2024/en

129 Fred Heiding, Alex O'Neill, and Lachlan Price, "Cybersecurity Strategy Scorecard", Belfer Center for Science and International Affairs", https://www.belfercenter.org/sites/default/files/2025-03/Cyber%20Strategy%20Scorecard_3.1.pdf.

gaps and challenges within strategy development and implementation and shares examples of good practice to navigate these challenges.

3.2. Key Observations

Participants highlighted the importance of aligning national frameworks with gender equality commitments. This involves gathering gender-disaggregated data, developing evidence-based policies, and ensuring that gender and gender-related threats are prioritized across the life cycle of digital and cybersecurity frameworks — to produce effective policies that serve all communities equally and do not perpetuate unequal power structures.

Awareness-raising, training, and education for national authorities working on cyber and digital policies emerged as a key best practice. Participants highlighted how regional and international initiatives, as well as initiatives by non-governmental stakeholders, can serve as roadmaps for developing good practices for gender-responsive cybersecurity as well as for reinforcing government efforts to integrate gender perspectives in national cybersecurity policies.

In Focus: Regional and International Efforts on Gender Mainstreaming in Cybersecurity Policies and Practices

The examples below illustrate how international organizations, regional bodies, and multilateral frameworks are embedding gender responsiveness into cybersecurity policy and practice. All these initiatives promote inclusive practices in training, risk management, and public–private partnerships and demonstrate how gender responsiveness can enhance not only domestic cyber resilience but also collective security through the cultivation of fair and inclusive global norms.

- **The Organization of American States' Cynder Project** works across Latin America and the Caribbean to integrate gender perspectives into national cybersecurity policies, build gender-sensitive capacity, and support the **Women in Cybersecurity Empowerment Network**.[130] The Network intended to "foster a gender-sensitive and inclusive regional cybersecurity culture" by bringing structural change and gender-sensitive advice back to participant organizations.
- At the EU level, the **European Cyber Security Organization's Women4Cyber** initiative promotes women's participation in cybersecurity through awareness-raising, networking, and retention efforts in the field.[131]

130 Organization of American States, "Cynder Project: Addressing the Gender Gap in the Cybersecurity Agenda of the Americas and the Caribbean", https://www.oas.org/ext/en/security/cynder-project.

131 Women4Cyber, https://women4cyber.eu/.

- **ITU** has included guidance on how to integrate gender considerations into national cybersecurity strategies in the updated edition of its **Guide to Developing a National Cybersecurity Strategy**.[132] The Guide suggests addressing the gender gap, promoting inclusion and gender equality in cybersecurity particularly through capacity development, workforce training, and addressing national-level skills gaps through equitable access to capacity-development opportunities.[133]
- **UNIDIR's work on gender and cybersecurity**, includes a range of research and policy recommendations. Related publications provide guidance on the integration of gender perspectives into cybersecurity governance,[134] explore the linkages between WPS Agenda and international cybersecurity,[135] and address the integration of gender considerations into the interpretation and implementation of the 11 norms of responsible State behaviour in cyberspace.[136]

3.3. Challenges and Gaps

Even with growing support and emerging good practices, participants noted several recurring obstacles that continue to limit the systematic integration of gender in national cybersecurity efforts. As shared by one participant, **"the main obstacles remain cultural bias, lack of data, and limited expertise — but treating gender as a cross-cutting principle, not a checkbox, has proven effective"**.

A primary concern is cultural bias existing within institutions in charge of cybersecurity and responsible for drafting and implementing NCSS. Cultural assumptions can shape how gender is perceived and prioritized and, in some contexts, discussions of gender itself may be considered socially or politically sensitive, further constraining the space for meaningful engagement on this issue. Practitioners emphasized that, in certain contexts, the mere introduction of gender as a framing mechanism may encounter resistance, limiting the extent to which it can be openly deliberated or operationalized within policy processes.

A distinct but related challenge arises even where cultural bias is less salient and political commitment to gender inclusion exists: the absence of a clear institutional mandate. Where no specific agency is assigned ownership of gender considerations within cybersecurity policy, responsibility remains diffused and commitments are not implemented. Gender references may be included nominally in strategy texts but go unsupported in practice — not always due to resistance, but because no institution has been tasked with driving them forward. This situation is further compounded by the lack of gender-disaggregated data, which limits the ability to build a comprehensive understanding of the issue and develop evidence-based policy responses.

132 ITU et al., "Guide to Developing a National Cybersecurity Strategy, 3rd Edition – Strategic Engagement in Cybersecurity", 2025, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.03-2025-PDF-E.pdf.

133 ITU, "CyberDrills", https://www.itu.int/en/ITU-D/Cybersecurity/pages/cyberdrills.aspx.

134 Katharine Millar, James Shires, and Tatiana Tropina, "Gender Approaches to Cybersecurity", UNIDIR, 2021, https://doi.org/10.37559/GEN/21/01.

135 Lisa Sharland, Netta Goussac, Emilia Currey, Genevieve Feely, Sarah O'Connor, "System Update: Towards a Women, Peace and Cybersecurity Agenda", UNIDIR, 2021, https://unidir.org/publication/system-update-towards-a-women-peace-and-cybersecurity-agenda/

136 Katharine Millar and Verónica Ferrari, "A Novel Approach to the 11 UN Norms for Responsible State Behaviour in Cyberspace: Guidelines for Gendered Implementation", Organization of American States; UNIDIR, 2025, https://unidir.org/publication/a-novel-approach-to-the-11-un-norms-for-responsible-state-behaviour-in-cyberspace-guidelines-for-gendered-implementation/

Moreover, sustained political commitment was considered essential for integrating and translating gender-related provisions in NCSS into concrete action. However, participants noted that the inclusion of gender language in national strategies and subsequent practical implementation often depends on institutional priorities or political leadership. Changes in priorities, limited institutional ownership, or the perception of gender as a secondary issue can weaken momentum for long-term integration and implementation efforts.

Further, participants noted that insufficient internal funding, coupled with a reliance on short-term or external funding, frequently limits institutional continuity and constrains efforts to operationalize gender considerations across policies' life cycles.

Finally, participants voiced concerns about the limited gender expertise among cybersecurity experts and gaps in community engagement. Many institutions responsible for cybersecurity policy development and implementation lack expertise on how to operationalize gender-responsive approaches. In consequence, agencies leading cybersecurity efforts may overlook broader societal considerations, including gender equality. Relatedly, discussions highlighted that technical cybersecurity actors often lack familiarity with gender analysis, while gender specialists are not always included in cybersecurity processes. In parallel, engagement with civil society, academia, grassroots organizations, and underrepresented communities often remains limited, reducing opportunities to incorporate diverse perspectives and lived experiences (including those of victims of ICT incidents) into policy design. This can result in strategies that overlook the differentiated impacts of cybersecurity threats and fail to address the needs of vulnerable or marginalized groups.

3.4. Good Practices, Lessons Learned, and Recommendations

Workshop discussions and desk research on NCSS and related policy efforts surfaced several common approaches, good practices and recommendations to integrate gender considerations into national cyber governance. While these approaches differ in detail across contexts, they provide practical pathways that States may adapt to their own institutional structures.

A. Harmonizing National Cybersecurity Frameworks and International Standards and Commitments

States have made wide-ranging commitments to gender equality across legal, policy, and normative frameworks — yet these commitments rarely find their way into NCSS.

Key Recommendations

- **Strengthen national legal and policy frameworks** by integrating a gender perspective to ensure protection of individuals and groups of individuals from cyberthreats.
- **Align cybersecurity frameworks with gender equality commitments** to ensure consistency across governance frameworks and to develop a comprehensive and effective policy ecosystem.

Participants stressed the need to strengthen national legal and policy frameworks by integrating a gender perspective to ensure protection of individuals and groups of individuals from cyberthreats. This can include adopting measures that account for the specificities of harms and disproportionate effects of cyber threats on the basis of gender. Examples included reflecting the specific and distinct features of gender-based violence and disinformation online and designing effective measures to address them, designing effective legal and administrative frameworks and redress mechanisms for victims,[137] and assigning equal weight to violations of human rights both online and offline.

Moreover, participants highlighted the added value of awareness-raising, training, and education of national authorities to ensure international standards and commitments are implemented with a gender perspective in mind, including by law enforcement, the judiciary, and national human rights institutions. Some practitioners pointed to different approaches to treatment of offline gender-based violence and online or technology-facilitated violence, which can lead to inconsistent responses from authorities. As one participant stressed, **"It is important to raise awareness at the national level of rising levels of technology facilitated gender-based violence, address the gap in perception, understanding and language and why it's important and should be treated as a threat to national security"**.[138]

Throughout the workshop, practitioners noted that integrating gender perspectives within NCSS can strengthen both their legitimacy and their effectiveness. Doing so ensures that cybersecurity policies protect all citizens, particularly women and marginalized groups, from cyberharms while enabling their greater participation in shaping cyber-resilience. As observed in chapter 1, gender inequalities persist across digital access, skills, and safety. When national strategies overlook such realities, they may risk perpetuating unequal power structures and producing solutions that do not serve all communities and individuals equally. Several examples shared on integrating gender equality considerations into cybersecurity policies are given in the following box.

137 See, for example, General Assembly, Promotion and Protection of the Right to Freedom of Opinion and Expression, A/76/258, 30 July 2021, paras. 64–67.
138 Participant in UNIDIR-Stimson Center workshops on gender mainstreaming in cybersecurity.

Good Practice: Aligning Cybersecurity Frameworks with Gender Equality Commitments

Embedding gender considerations into NCSS can support more comprehensive risk analysis by reflecting the lived realities of groups. Some examples shared of States that have made explicit efforts to align cybersecurity priorities with gender equality commitments are the following.

- The **2023 National Cybersecurity Strategy of Canada** links its digital governance priorities to the State's broader gender equality commitments. The strategy adopts a 'whole-of-society' approach to strengthen cyber capacity through awareness campaigns and investment in diverse cybersecurity talent acquisition.[139]
- The **2022 Cybersecurity Policy of Costa Rica** emphasizes inclusive participation and digital literacy for all citizens.[140] For example, it stresses that all digital literacy initiatives must take into account key cross-cutting elements, namely a gender perspective and the need to reach the most vulnerable members of the population.
- The **2026 National Cybersecurity and Resilience Strategy of Fiji** focuses on building cyber-aware and digitally safe communities, emphasizing digital literacy trainings and expanding equitable participation in the digital economy.[141] Among its priorities, the strategy stresses the goal to close the gender gap in the cybersecurity workforce and to promote women, youth, and underrepresented groups in cybersecurity careers.[142] It also aims at advancing the WPS Agenda in all forums and adopts a viewpoint that "all human security includes women's security".[143]

B. Inclusive Participation, Multi-Stakeholder Consultation and Workforce Development

Developing gender-responsive cybersecurity strategies depends not only on what is written into policy, but on who shapes it. Broadening participation throughout the strategy development cycle — from consultation to implementation — brings in a broad range of perspectives and expertise.

139 Government of Canada, "Canada's National Cyber Security Strategy", 2025, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx.

140 Costa Rican National Cybersecurity Strategy 2023–2027, https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20 Costa%20Rica%20-%20 10Nov2023%20ENG.pdf.

141 Riya Mala, "Cabinet Endorses Fiji's National Cybersecurity Strategy 2026–2031", 5 February 2026, https://www.fbcnews.com.fj/news/cabinet-endorses-fijis-national-cybersecurity-strategy-2026-2031/.

142 See Ministry of Policing and Communications of Fiji, "National Cybersecurity and Resilience Strategy 2026 – 2031", 18 March 2026, https://demo.fijianmade.gov.fj/.

143 Ministry of Social Welfare, Women and Poverty Alleviation of Fiji, "Fiji National Gender Policy", https://wrd.unwomen.org/sites/default/files/2022-06/1%20National%20Gender%20Policy-%20FIJI_0.pdf.

Key Recommendations

- **Ensure meaningful participation in the cybersecurity strategy development process** to include experiences and priorities that may not be visible in purely technical forums, thereby broadening the evidence base for setting national objectives and conducting risk assessments.
- **Plan inclusive consultations** by outlining the stakeholders to be consulted, and use multiple formats (such as written inputs, roundtables, and online platforms) to enable participation by actors with differing capacities. Consider consultations with groups that may face specific barriers or harms, such as women journalists, human rights defenders, and rural communities.
- **Develop education programmes** that invest in training women and other underrepresented groups in cybersecurity leadership to broaden participation, strengthen local expertise, and promote innovation.

Participants highlighted that the broader community of stakeholders can contribute important good practices for gender-responsive cybersecurity that can complement and reinforce government efforts. Civil society organizations have developed practical tools that can help governments and other actors to embed gender analysis and human rights considerations in cybersecurity policy cycles, and to design more inclusive processes for cyber norm development and implementation. Several initiatives discussed in the following box illustrate how stakeholders beyond government can operationalize gender mainstreaming by building shared analytical tools, fostering values-based dialogue, and creating feedback loops between community experience and policy design, thereby strengthening both the substance and the legitimacy of national and international cybersecurity governance.

Good Practices: Multi-Stakeholder Initiatives on Gender Mainstreaming in Cybersecurity

- **The Association for Progressive Communications' framework** for developing gender-responsive cybersecurity policy offers: (i) an assessment tool with step-by-step advice and concrete recommendations;[144] (ii) a compendium of relevant norms, standards and guidelines, including the assessment of international legal and normative instruments such as the CEDAW, the Beijing Declaration and Platform for Action, the WPS Agenda, the 2030 Agenda for Sustainable Development, the Human Rights Council reports and resolutions, and the United Nations cybersecurity processes;[145]

144 APC, "A framework for developing gender-responsive cybersecurity policy: Assessment tool", 2023, https://www.apc.org/sites/default/files/apcgendercyber-assessmenttool.pdf

145 APC, "A framework for developing gender-responsive cybersecurity policy: Norms, standards and guidelines" 2022, https://www.apc.org/sites/default/files/gender-cybersecurity-policy-norms.pdf

and (iii) a literature review which provides context, and defines specific concepts related to gender and cybersecurity.[146] Together, these elements help stakeholders to diagnose gendered risks, map applicable international commitments, and identify concrete entry points for reform.[147] It encourages policymakers, regulators, and advocacy groups to:

- systematically apply intersectional gender analysis to threat modelling and incident response;
- integrate gender-disaggregated data collection into cybersecurity baselines and impact assessments;
- ensure that consultation processes meaningfully include women's rights, gender, youth, and digital rights organizations; and
- treat cybersecurity as a public interest and human rights issue rather than a purely technical or securitized domain.

- **Global Partners Digital's Toolkit for Inclusive and Value-Based Cybersecurity Policymaking** provides practical guidance for structuring multi-stakeholder engagement around clear normative principles, such as transparency, accountability, non-discrimination, and openness. It further provides guidance on designing participatory mechanisms that enable affected communities, technical experts, private sector actors, and human rights advocates to shape national positions and cyber norms.[148] It offers templates and checklists for inclusive consultations, guidance on integrating civil society evidence into national strategies and international negotiations, and examples of how non-State actors can monitor implementation and hold governments and companies accountable for gender-related cyberharms.[149]

Additionally, participants emphasized inclusive participation in cyber policy design and the cultivation of a more diverse cybersecurity workforce. Participants stressed that engagement should go beyond numerical representation and engage different perspectives in the decision-making process.[150] As put by one practitioner in the workshops, there is a need to **"push to be accommodated, not just included"**.

Meaningful participation in the strategy development process makes it possible to surface experiences and priorities that may not be visible in purely technical forums, thereby broadening the evidence base for setting national objectives and conducting risk assessments. As observed by one participant in the workshops, **"if half of the world is left out of cybersecurity, half of the solutions are missing"**. States can promote this process by supporting girls in science, technology, engineering, and mathematics

146 APC, "A framework for developing gender-responsive cybersecurity policy: Literature review" 2022, https://www.apc.org/sites/default/files/gender-cybersecurity-policy-litreview.pdf

147 Association for Progressive Communications, "A Framework for Developing Gender-Responsive Cybersecurity Policy", 2023, https://www.apc.org/en/pubs/framework-developing-gender-responsive-cybersecurity-policy.

148 Global Partners Digital, "Toolkit for Inclusive and Value-Based Cybersecurity Policymaking", 26 August 2020, https://www.gp-digital.org/publication/toolkit-for-inclusive-and-value-based-cybersecurity-policymaking/.

149 Ibid.

150 UN Women, "Implementation of the Beijing Declaration and Platform for Action Netherlands Review Report", 2019, https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/CSW/64/National-reviews/Netherlands.pdf.

disciplines and in cybersecurity through education and training programmes, which can be reflected in dedicated NCSS sections on capacity-building or workforce development.

Good Practices: The Empowerment of Women in Cybersecurity

- **Malawi** has included women in drafting and assessment processes and, building on the momentum generated through its participation in the **Women in Cyber Fellowship**, has created a "women and girls in cyber" conference as a platform for capacity-building and mentorship.[151]
- **Thailand's National Cyber Security Agency** organizes initiatives such as **Women Thailand Cyber Top Talent**[152] to promote mentorship, create an inclusive leadership pipeline, enhance visibility of women in cybersecurity roles, and showcase gender inclusivity as a driver of resilient cybersecurity.[153]

C. Institutional Mandates for Gender Mainstreaming

Participants highlighted that even where political will exists, progress on integrating gender into cybersecurity frameworks is frequently undermined by the absence of clear institutional mandates. Without a designated entity formally empowered and accountable for gender mainstreaming, efforts can remain fragmented and vulnerable to political or funding shifts. Participants stressed that assigning clear mandates and embedding gender focal points within relevant decision-making bodies is necessary for translating political commitments into sustained action.

Key Recommendations

- Designate a ministry, institution, department, agency, or focal point as the **entity responsible for gender mainstreaming in technology governance and integrate them in other national cyber policy-setting and decision-making processes**. Clear mandates prevent fragmentation and improve coordination during crisis or policy review.
- Strengthen collaboration between **cybersecurity institutions and governmental offices or focal points** tasked with advancing gender equality, where such entities exist.
- Ensure that cybersecurity strategies are **aligned with broader development objectives**, including gender equality goals, and seek high-level integration of gender and digital priorities across government through effective inter-agency coordination to reduce fragmentation, align resources, and create shared incentives for gender-responsive cyber policies.

151 "MACRA host Women in Cyber Conference", 16 August 2025, MACRA, https://macra.mw/macra-host-women-in-cyber-conference/
152 See Thai National Cyber Academy, "Women Thailand Cyber Top Talent", https://www.thnca.or.th/fiscal-2568/wtctt2025/.
153 Survey respondent for UNIDIR-Stimson Center workshops on gender mainstreaming in cybersecurity.

Participants also highlighted the value of strengthening collaboration between cybersecurity institutions and governmental offices or focal points tasked with advancing gender equality. Where such entities exist, practitioners noted that such collaboration can promote consistency across national gender policies and cybersecurity agendas, and enable gender expertise to inform cyber strategy development, implementation, and review. One approach that was shared was to designate a government institution with gender expertise to review draft cybersecurity strategies and contribute to regular implementation assessments, without changing the core mandates of the existing authority.[154] Participants further emphasized the necessity of embedding gender equality as a high-level priority across government, connecting cybersecurity strategy to broader development and national security objectives, rather than being confined to a single agency.

Good Practices: Effective Coordination Among Relevant Structures

- In **Rwanda**, the Ministry of ICT and Innovation cooperates closely with the Prime Minister's Gender Monitoring Office, which is responsible for monitoring compliance with gender commitments across public and private sector entities. The two offices collaborate to collect gender-disaggregated data on digital access and safety and to conduct regular audits of women's participation in ICT and cybersecurity education.[155]
- In **Chile**, gender and digital policy priorities are integrated at a high level within national governance structures. The Ministry of Women and Gender Equity, part of the presidential strategic cabinet, helps to align national strategies across sectors.[156] Chile's second WPS Agenda NAP explicitly recognizes digital safety and technology governance as priorities for promoting inclusive security,[157] while the Digital 2035 strategy addresses digital gender-based violence and access to infrastructure.[158] Chile's National Cybersecurity Strategy was developed and implemented with input from a variety of ministries across government and in consultation with civil society and grass roots organizations,[159] and its recommendations are informing regulatory updates and capacity-building efforts to expand secure digital access nationwide.
- **Fiji's National Gender Policy** aims at improving awareness among policymakers, planners, implementers and the general public about instruments related to gender and their implementation, including the implementation of national cybersecurity commitments as part of the "all human security includes women's security" approach.[160]

154 Global Forum on Cyber Expertise, "Mainstreaming Gender in Cyber Capacity Building", 2022, https://thegfce.org/wp-content/uploads/GFCE-Concept-Note-on-Mainstreaming-Gender-In-Cyber-Capacity-Building-2.pdf.

155 See Gender Monitoring Office of Republic of Rwanda, "Gender Profile in Information and Communication Technology", 2017, https://www.migeprof.gov.rw/fileadmin/user_upload/Migeprof/Publications/Reports/Gender_Profile_in_ICT_Sector_Booklet-March_2017.pdf

156 Organisation for Economic Co-operation and Development, "Implementing Chile's National Digital Identity Strategy", 2 December 2025, https://www.oecd.org/en/publications/implementing-chile-s-national-digital-identity-strategy_04a67b8b-en/full-report/component-4.html.

157 SecurityWomen, https://www.securitywomen.org/unscr-1325-and-national-action-plans-nap/chile-2.

158 Estrategia de transformación digital Chile Digital 2035, https://doc.ingenieros.cl/telco_estrategia_chiledigital.pdf.

159 Stephania Alvarez, "Chile: Framework Law on Cybersecurity Comes into Force", 30 January 2025, Global Legal Monitor, https://www.loc.gov/item/global-legal-monitor/2025-01-30/chile-framework-law-on-cybersecurity-comes-into-force/.

160 Ministry of Social Welfare, Women and Poverty Alleviation of Fiji, "Fiji National Gender Policy", https://wrd.unwomen.org/sites/default/files/2022-06/1%20National%20Gender%20Policy-%20FIJI_0.pdf.

D. Gender-Responsive Reporting Mechanisms

Practitioners strongly reinforced the importance of the development of gender-responsive cyber incident reporting and response mechanisms that are responsive to gender-specific harms and barriers, including technology-facilitated gender-based violence. NCSS increasingly reference the need for accessible, trusted channels through which individuals can report cyber incidents, including harassment, doxing, and other forms of online abuse.[161] Some NCSS establish general principles for such mechanisms and platforms, such as providing multiple reporting channels, protecting privacy and data security, and making trained staff available — while leaving detailed institutional design to specialized agencies. One participant noted that some States have also "accounted for online harassment and stalking explicitly in legislative powers by strengthening protection for victims and enabling authorities to prosecute offenders more effectively."[162]

Key Recommendations

- **Enable gender-responsive cyber incident reporting and response mechanisms** that consider gendered harms and barriers, including TFGBV.
- **Design accessible and trusted reporting mechanisms for cyber incidents** that include general principles such as multiple reporting channels, confidentiality, privacy protection, and trained staff to handle sensitive cases. Where appropriate, specialized units or channels may be considered by relevant authorities, for instance personnel of different genders (cf Pakistan example that follows).

Good Practices: Strengthening Frameworks and Mechanisms to Report TFGBV

The following examples were shared during the workshop to illustrate various efforts in this regard.

- In **Pakistan,** some police stations are staffed by women to facilitate round-the-clock reporting by those who may be reluctant to disclose incidents to male officers, particularly in cases of TFGBV.[163]
- **Armenia** has developed a police-run chat where children can report concerns online and receive rapid responses, as well as apps to help women to report gender-based violence.[164]

161 Simone Busetti and Francesco Maria Scanni, "Evaluating Incident Reporting in Cybersecurity: From Threat Detection to Policy Learning", *Government Information Quarterly*, vol. 42, no. 1, 2025, https://doi.org/10.1016/j.giq.2024.102000.

162 Survey respondent for UNIDIR-Stimson Center workshops on gender mainstreaming in cybersecurity.

163 Ashfaq Ahmed, "Helpline 1815: Pakistan Launches First Women Only Digital Police Station", 24 July 2025, Gulf News, https://gulfnews.com/world/asia/pakistan/helpline-1815-pakistan-launches-first-women-only-digital-police-station-1.500209874.

164 Zara Sargsyan, "The First Online Cybersecurity Platform for Children and Adolescents Launched in Armenia", 27 August 2025, United Nations Armenia, https://armenia.un.org/en/300934-first-online-cybersecurity-platform-children-and-adolescents-launched-armenia; Svetla Baeva, "SafeYOU, an Armenian App, Is Taking on Gender-Based Violence Around the World", 8 December 2022, UNDP Innovation Community in Europe and Central Asia, https://innovation.eurasia.undp.org/safeyou-an-armenian-app-is-taking-on-gender-based-violence-around-the-world/.

- **Ireland** strengthened legal frameworks to support complaints by individuals on harmful online content and harassment.[165]
- **Australia** has developed a platform to report TFGBV for investigation, including adult cyberabuse, cyberbullying, and image-based abuse.[166]

E. Gender-Sensitive Monitoring and Review Mechanisms

Another featured approach in the discussions centred on integrating gender-responsive indicators and monitoring arrangements into NCSS and implementation frameworks. Specifically, incorporating gender-disaggregated data and gender-sensitive evaluation criteria and indicators into regular reviews of NCSS implementation can help States to understand how different groups experience digital threats and the impacts of cyber policies over time. Findings can be used to inform subsequent strategy updates.

Key Recommendations

- **Collect and use gender-disaggregated data** for developing cybersecurity policies, including on access to digital infrastructure, types of incidents, and use of reporting mechanisms.
- **Ensure regular monitoring and evaluation for cyberpolicies using gender-sensitive indicators** within the broader monitoring framework of cybersecurity strategies, and specify who is responsible for collecting and analysing this information.
- **Establish periodic reviews or audits** that consider how different groups experience digital threats and how this information will inform subsequent strategy updates.

Good Practices: National Practices on Gender Assessments

The following examples were given of States that conduct gender assessments as part of their national practices

165 See, for example, Ireland's Harassment, Harmful Communications and Related Offences Act 2020, Harassment, Harmful Communications and Related Offences Act 2020https://www.irishstatutebook.ie/eli/2020/act/32/enacted/en.

166 See, eSafety Commissioner of Australia, "What you can report to eSafety", https://www.esafety.gov.au/report/what-you-can-report-to-esafety.

- **Ukraine** conducts regular gender audits to assess progress over time across all institutions responsible for information protection.[167]
- **Uganda's** national development planning framework integrates cybersecurity within a wider digital transformation agenda and uses gender-disaggregated data from the research and planning directorate to inform capacity-building.[168]
- **Rwanda's National Cybersecurity Agency** supports the periodic assessment process under the National Gender Policy designed to review the implementation of gender goals across sectors.[169]

F. Institutional Lessons from the WPS Agenda

The integration of gender within NCSS can also draw upon the institutional lessons of the WPS Agenda. Participants highlighted that national and regional action plans developed under WPS Agenda can provide useful models for interministerial coordination, public consultation, and performance measurement, and can serve as national blueprints for implementing international commitments. The same applies to broader national strategies on the prevention of violence against women, among other frameworks that may overlap across contexts.

Linking these frameworks with cybersecurity strategies, especially in addressing digital threats such as online gender-based violence or cyber-enabled disinformation targeting women, can create greater coherence across traditional and digital security domains. In turn, these frameworks can evolve to reflect the reality of digital threats. For example, as of now cyberthreats remain largely absent from current action plans.[170] One participant pointed to a programme in Asia that supports States in developing NAPs that integrate non-traditional issues, including NCSS.

Key Recommendations

- Build **models for interministerial coordination, public consultation, and performance measurement** of WPS Agenda NAPs that can serve as national blueprints for implementing international commitments.

167 UN Women, "Gender Audit in Action: Ukraine Strengthens Institutional Capacity for Gender-Responsive Recovery", 17 October 2025, https://ukraine.unwomen.org/en/stories/pres-reliz/2025/10/hendernyy-audyt-v-diyi-ukrayina-zmitsnyuye-instytutsiynu-spromozhnist-dlya-henderno-vidpovidalnoho-vidnovlennya.

168 Ministry of ICT and National Guidance of Uganda, "Digital Transformation Roadmap 2023/2024 - 2027/2028", https://ict.go.ug/site/documents/Digital%20Transformation%20Roadmap.pdf; Republic of Uganda, "National Cybersecurity Strategy", 2022–2026, https://dig.watch/resource/ugandan-national-cybersecurity-strategy-2022-2026https://ict.go.ug/site/documents/National-Cybersecurity-Strategy-UG.pdf.

169 See Ministry of Gender and Family Promotion of Rwanda, "Revised National Gender Policy", 2021, https://www.migeprof.gov.rw/fileadmin/user_upload/Migeprof/Publications/Guidelines/Revised_National_Gender_Policy-2021.pdf.

170 Civil Society Alliances for Digital Empowerment, "APC Report Finds Digital Risks Largely Absent from Global Women, Peace and Security Action Plans", 3 December 2025, https://cadeproject.org/updates/apc-report-finds-digital-risks-largely-absent-from-global-women-peace-and-security-action-plans/.

- **Link these frameworks with cybersecurity strategies**, especially in addressing digital threats such as TFGBV and online gendered disinformation to ensure coherence across traditional and digital security domains.
- **Integrate online dimensions to components on prevention and response to sexual and gender-based violence** in WPS Agenda NAPs and tailor prevention and response accordingly.[171]

Good Practices: National and Regional Action Plans including References to Cybersecurity Elements

The following selected examples were shared during the workshop of national and regional action plans for the implementation of the WPS Agenda.[172]

- The **ASEAN Regional Plan of Action on WPS** includes within its approaches the engagement of women in emerging security issues, including in the digital space. Within its priority actions it includes closing the gender digital divide, as well as mitigating the risks of online gender-based violence.[173]
- **Malaysia's NAP** explicitly includes protecting women in cybersecurity as part of its pillars.[174]
- **Colombia's NAP** includes specific actions related to training on cybersecurity and prevention of gender-based violence in all its forms, as well as awareness-raising on digital security. It also includes concrete actions on reducing the gender digital divide.[175]
- The **United Kingdom's NAP** addresses cybersecurity threats affirming that "gender considerations must be at the forefront of the global response to cyber threats".[176] It includes concrete references to addressing the gender digital divide and promoting responsible inclusive digital spaces as part of addressing online gender-based violence.[177]

---

171 See International Committee of the Red Cross, Nordic Centre for Gender in Military Operations, and Swedish Red Cross, "International Humanitarian Law and a Gender Perspective in the Planning and Conduct of Military Operations", March 2024, https://shop.icrc.org/international-humanitarian-law-and-a-gender-perspective-in-the-planning-and-conduct-of-military-operations-pdf-en.htmlhttps://shop.icrc.org/download/ebook?sku=4741/002-ebook, pp. 37 and 39. Note that this list is not cyber-specific and is included here as a general indication of where cyber-related adaptations or edits could be considered.

172 For a broader overview of NAPs including references to cyber, see https://www.wpsnaps.org/; see also Myrttinen Henri, Anastaesia Mondesir, and Mariana Terreros Lozano, "Toolkit: Addressing Weapons-Related Risks in Women, Peace, and Security National Action Plans," UNIDIR, 2026, https://unidir.org/publication/toolkit-addressing-weapons-related-risks-in-women-peace-and-security-national-action-plans/

173 See "ASEAN Regional Plan of Action on Women, Peace and Security", https://www.asean.org/wp-content/uploads/2022/11/32-ASEAN-Regional-Plan-of-Action-on-Women-Peace-and-Security.pdf.

174 See UN Women Asia and the Pacific, "National Action Plans: Women, Peace and Security", https://asiapacific.unwomen.org/en/focus-areas/peace-and-security/national-action-plans. See in particular Ministry of Women, Family and Community Development of Malaysia, "National Action Plan on Women, Peace and Security 2025-2030", 2025, https://asiapacific.unwomen.org/sites/default/files/2025-10/Malaysia%27s%20National%20Action%20Plan%20on%20Women%2C%20Peace%20and%20Security_compressed.pdf.

175 See Republic of Colombia, "Primer Plan de Acción Nacional Mujeres, Paz y Seguridad: Resolución 1325 del Consejo de Seguridad de las Naciones Unidas", https://wpsfocalpointsnetwork.org/wp-content/uploadses-397916_recurso_2.pd/2025/01/articlf.; see also, Association for Progressive Communications, "The Missing link: Cybersecurity and technologyTechnology-facilitated Gender-based Violence in the Women, Peace and Security Agenda", 2025, https://www.apc.org/sites/default/files/the-missing-link.pdf.

176 See Government of the United Kingdom, "UK Women, Peace and Security National Action Plan 2023-2027", https://assets.publishing.service.gov.uk/media/645d2d94ad8a03001138b33c/uk-women-peace-security-national-action-plan-2023-2027.pdf, p. 29.

177 Ibid.

- **Kenya's NAP**[178] highlights cybersecurity and AI as emerging priorities. It explicitly states the need to strengthen gender-sensitive digital legislation and enforcement, work on expanding prevention and response to TFGBV, embed WPS principles into cybersecurity and AI strategies, invest in women's digital literacy, and "adopt proactive measures to combat disinformation and online backlash particularly during elections".[179]

178 See Ministry of Gender, Culture and Children Services of Kenya, "Kenya National Action Plan 2025-2029", https://africa.unwomen.org/sites/default/files/2025-11/knap_iii_2025-2029_0.pdf.

179 Ibid., p. 16.

4. Gender-Responsive Cyber Capacity-Building

4.1. Introduction

Developing inclusive and effective cybersecurity policies requires not only technical expertise, but also the ability to reflect the diverse realities of those affected by cyber threats. Gender-responsive cyber capacity-building (CCB) has therefore emerged as a critical enabler of both meaningful participation and more resilient cybersecurity systems. While there is no universal definition of 'gender-responsive cyber capacity-building', programmes designed to respond to gender considerations can materialize in two ways:

- they can respond to the underrepresentation of different groups in cybersecurity such as women and gender minorities; or
- they can include substantive elements to mainstream gender within cybersecurity processes for a broader range of stakeholders.

These two approaches often intersect, and such programmes can adopt a blended approach where, for instance, they may be designed for women professionals and also include material on integrating gender and human rights considerations in cybersecurity policies and practices. Furthermore, capacity-building is highlighted in the UN framework for responsible State behaviour in cyberspace, especially with the 2025 final report of the **Open-ended Working Group (OEWG)** in July 2025, as a central and cross-cutting pillar.[180] Over the past few years, efforts to better include women professionals in particular in the various strands of work on cybersecurity have steadily increased in scale, scope, substance and stakeholder base.

This chapter examines the intricacies of gender-responsive CCB initiatives both at the systemic level as well as through specific examples. It underlines some of the key observations participants made on the CCB programmes that they were familiar with, as well as some of the challenges that they face as the trainers and recipients of these programmes. Supported by an evidence-based analysis through the examples cited in the workshop, the chapter concludes with a set of actionable recommendations.

4.2. Key Observations

Participants highlighted that gender-responsive CCB initiatives respond to persistent gaps and blind spots in system design, policy development, threat assessment, and incident response, while also addressing the differentiated ways in which cyber threats are experienced. A range of initiatives across global, regional, and national levels were discussed, and the discussion centred on a needs-based

180 See General Assembly, Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, A/AC.292/2025/CRP.1, 11 July 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_10_July_2025.pdf.

approach to capacity-building. Participants also emphasized the value of contextualized approaches, tailoring programmes to specific national, institutional, and sectoral needs, and of multi-stakeholder engagement involving governments, international organizations, civil society, and industry.

Gender-responsive CCB was perceived as not only a matter of fairness, but also necessary for effective cyber resilience — human security is as equally important as the security of devices, networks, and infrastructure, and this can include differentiated approaches towards the security of women, men, girls, boys, and individuals of diverse gender expressions. Participants highlighted that if we do not design CCB programmes contextually for different groups and identities, then this neutrality can overlook structural inequalities, and potentially even worsen them.

4.3. Challenges and Gaps

Through a discussion rooted in an aggregate of realistic situations, participants identified several persistent limitations in integrating gender within CCB initiatives. A primary concern is the lack of sustained and predictable funding, which undermines the continuity and long-term impact of capacity-building programmes. Institutional barriers also remain significant, including limited recognition of structural challenges affecting the recruitment and retention of women in cybersecurity professions, and broader workforce disparities.

Participants further cautioned against tokenistic approaches, where gender considerations are included superficially, either through minimal representation targets or limited integration in programme content, without addressing deeper structural issues. The absence of intersectional approaches can also result in the exclusion of certain groups, including gender minorities, young people, and individuals from marginalized socioeconomic or geographic backgrounds. Finally, gaps in monitoring and evaluation were highlighted, with the limited use of disaggregated data and feedback mechanisms constraining the ability to assess impact, avoid duplication, and refine relevant capacity-building programming over time.

4.4. Good Practices, Lessons Learned, and Recommendations

The insights and examples of good practices gathered from desk-based research and the workshops have been distilled below and organized into sections grouping similar approaches together. While representative in terms of providing evidence-based and experience-backed recommendations, the following is not exhaustive.

A. Avoiding Tokenistic Approaches to Gender-Responsive CCB

Participants brought up the importance of concrete actions and avoiding tokenistic approaches several times, stressing that doing so is critical to ensuring the longevity and impact of CCB programmes. Failing to do so may lead to widening the gap between opportunity and talent, which is what gender-responsive CCB initiatives intend to bridge.

Key Recommendations

- **Ensure gender-responsive CCB programmes are continually included** in evolving policy documents, strategies, forums, and plans on cybersecurity. Concrete mentions of gender-responsive capacity-building in relevant frameworks form **a strong basis for fundraising and resource mobilization** and reinforce that such capacity-building cannot be brushed aside as a 'nice to have' optional approach.
- **Ensure that CCB initiatives reach and represent the right stakeholders** in relevant roles and positions. Tokenistic inclusion of experts and topics on gender mainstreaming in such programmes was seen by the participants as performative, as if gender were merely an afterthought or a checkbox.

The **Women in Cyber Fellowship** is an oft-cited example of a CCB programme designed for the right group of policy actors, and its success has resulted in the recognition of gender-responsive CCB programmes as a good practice in important policy outputs.

Good Practice: Women in International Security and Cyberspace Fellowship

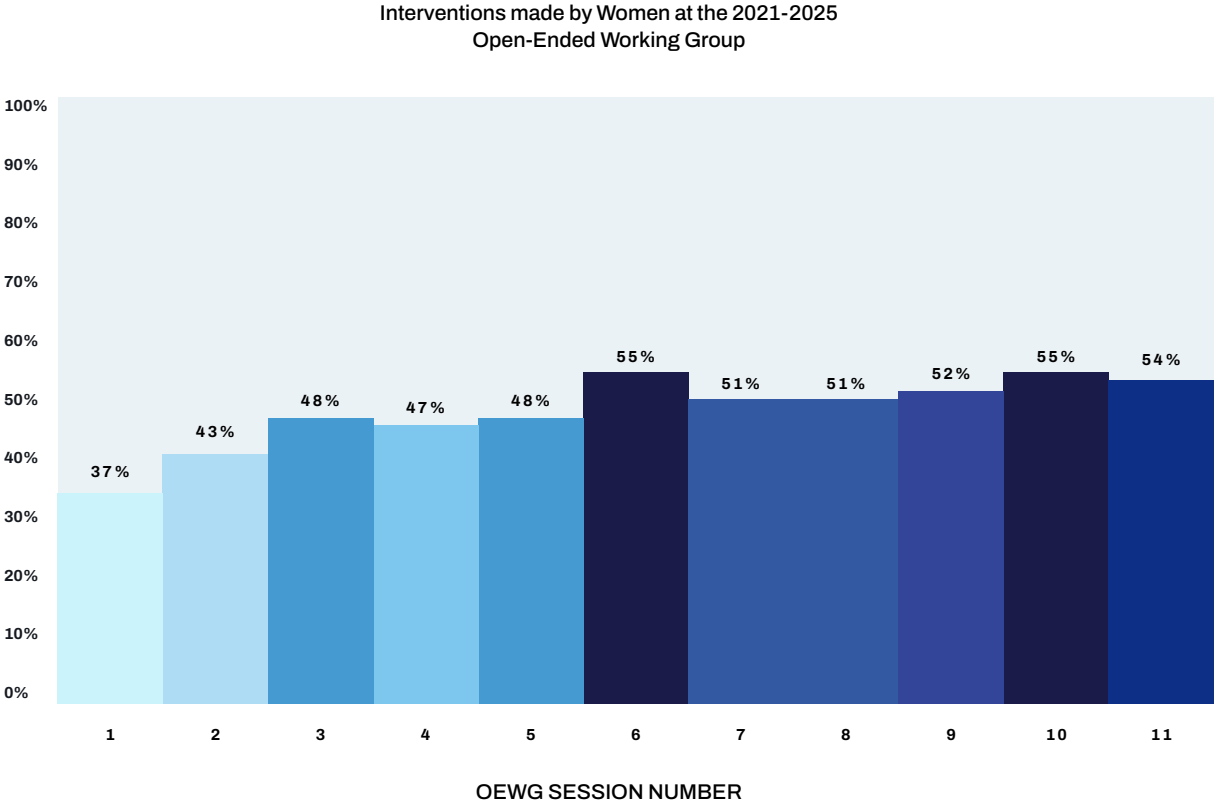
Launched in February 2020, the Fellowship is a capacity-building and institutional support programme coordinated at various times by the Global Forum on Cyber Expertise, the United Nations Institute for Training and Research, and currently by UNIDIR.[181]

The WiC Fellowship strengthens the skills and knowledge of a group of women delegates and leaders in cybersecurity from all regions, since the UN General Assembly First Committee has the lowest proportion of women diplomats out of the UNGA's Main Committees.[182] It adopts a blended approach to gender-responsive CCB and conducts a training programme for women delegates before every session of the OEWG, featuring substantive elements about cybersecurity. The Fellowship has trained over 120 women diplomats from more than 55 underrepresented States in the OEWG.

181 Global Forum on Cyber Expertise, "Women in International Security and Cyberspace Fellowship", https://thegfce.org/project/women-in-international-security-and-cyberspace-fellowship/. The UN Institute for Training and Research (UNITAR) and UNIDIR have been knowledge partners for different editions of the Fellowship during the recently concluded OEWG.

182 Renata Hessmann Dalaqua, Kjølv Egeland, and Torbjørn Graff Hugo, "Still Behind the Curve: Gender Balance in Arms Control, Non-proliferation and Disarmament Diplomacy", UNIDIR, 2019, https://unidir.org/wp-content/uploads/2023/05/Still-behind-the-curve.pdf.

The WiC Fellowship is often cited as a successful example of gender-responsive CCB, evidenced by the remarkable increase in women's participation and leadership at the OEWG, which was explicitly acknowledged by Member States in the final 2025 OEWG report.[183] During the 11th and final substantive session of the OEWG in July 2025, women delivered 54 per cent of all interventions, becoming one of the only processes on international security in the UN to reach gender parity (see figure below).



***Source**: Data collected from the statements made by the Australian delegation on the agenda item 'Any other business'* [184]

Apart from the structural success of the full and meaningful inclusion of more women in the OEWG process, the cascading effects of the WiC Fellowship have also indirectly facilitated gender-related considerations in OEWG discussions and final documents. The impact of such CCB programmes extends beyond any one engagement in multilateral negotiations.

183 General Assembly, Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, A/AC.292/2025/CRP.1, 11 July 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_10_July_2025.pdf, para. 53(k).

184 See OEWG, Australian Statement on Gender Representation, 11 July 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Australian_Statement_OEWG11_Gender_Representation_11_July_2025_Final.pdf; see also Statement by the representative of Australia to the Seventh substantive session of the OEWG, March 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OWEG_7_-_Australian_intervention_-_Other_business_-_gender_-_March_2024.pdf; Statement by the representative of Australia to the Fourth substantive session of the OEWG, March 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG4_-_Australia_intervention_-_Other_business_(gender)_-_March_2023.pdf; for additional information see https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/gender_data_stats.pdf

B. Institutionalizing Monitoring and Evaluation and Sharing Good Practices

A nuanced approach to monitoring and evaluation was cited by participants as a key requirement to fully realize the potential of gender-responsive CCB programmes. In terms of internal monitoring, understanding which indicators would be relevant to report on and thus proper to track is essential. For evaluation and strategic prioritization, participants considered it useful to include outcomes of CCB initiatives beyond numbers of programmes delivered and practitioners trained, such as tangible policy impact, leadership of women experts, and branding of gender-responsive CCB programmes. Since such approaches require financial support, involving wider audiences for capacity-building and establishing a mechanism to share good practices were recommended in order to encourage higher funding.

Key Recommendations

- **Support, institutionalize, and adequately fund** gender-responsive capacity-building programmes to ensure long-term impact. This can be **supplemented by monitoring and evaluating programmes** to inform future programming, through tracking positive impacts and cascading effects over time to demonstrate value, identifying evolving needs and gaps, and avoiding duplication of efforts.
- **Encourage the sharing of lessons learned and good practices** on gender-responsive CCB across the multi-stakeholder community to strengthen collective impact. Since cybersecurity as a domain of activity is continuously evolving due to new technologies and policy imperatives, the **establishment of effective feedback loops can help capacity-building programmes to remain relevant and productive**.

Participants highlighted that successful CCB initiatives have usually been institutionalized and adequately funded multi-year programmes. For instance, **Australia, Canada, Germany, the Netherlands, New Zealand, the United Kingdom, and the United States** have funded and supported the Women in Cyber Fellowship for the past several years, in addition to other global and regional gender-responsive CCB programmes.

In terms of monitoring and evaluation, participants highlighted that a robust framework tracking the background and impact of CCB initiatives can help to improve not only the programmes themselves but also consequent policies and related engagements. An example mentioned was **Canada**'s[185] use of a systemic and intersectional approach rooted in its **GBA Plus** framework to keep track of its activities and projects on cybersecurity and several other substantive issues. GBA Plus is an analytical tool that considers how various factors (e.g., age, race, disability, geography) intersect to shape experiences with various policies.[186] As a tool that all government employees are trained on, GBA Plus helps to analyse

185 Global Affairs Canada's engagement in the UNIDIR–Stimson Center workshop and written response to the corresponding survey.

186 Government of Canada, "Gender-based Analysis Plus (GBA Plus)", https://www.canada.ca/en/women-gender-equality/gender-based-analysis-plus.html.

cybersecurity threats through a gendered lens and mainstream gender in Canadian cyber policies, and is employed in the context of capacity-building and the provision of support.

C. Prioritizing Research for and Contextualization of CCB Programmes

The first step to creating successful CCB programmes is conducting in-depth research in order to develop foundational training materials. Workshop participants highlighted that the principle of 'do no harm' should also be a standard approach in capacity-building around cybersecurity, especially considering contextual sensitivities for the target audience, sector, country and/or region.

Key Recommendations

- **Prioritize and fund research to address existing knowledge gaps** on effective gender-responsive CCB programming and to inform evidence-based approaches. Gender-responsive capacity-building programmes also benefit from **strengthening the link between research and implementation** to ensure that training content reflects real-world challenges and emerging threats.
- **Incorporate research on gendered ICT-related harms** into CCB programmes, and **to** contextualize CCB programmes so that they are **designed for the target communities of practice, levels of cyber maturity, institutional needs, and national, regional and cultural specificities**. Gender-responsive programmes that are aligned with relevant national and international frameworks on cybersecurity were observed to have more coherence and policy relevance.

Apart from the establishment of gender-responsive CCB programmes, participants stressed the need for research to provide foundational material for CCB programmes. **UNIDIR** conducts research on the incorporation of gender considerations throughout international cybersecurity policy and practice,[187] and has specifically addressed the gendered implementation of the 11 norms of responsible State behaviour in cyberspace, which includes cyber capacity-building.[188] In UNIDIR's tailored bilateral national and regional CCB workshops, this research has been used to mainstream gender through inclusion of topics such as TFGBV, the integration of gender in national cybersecurity policies and practices, and implementation of the WPS Agenda by including cyber and digital issues in NAPs.[189]

187 Katharine Millar, James Shires and Tatiana Tropina, "Gender Approaches to Cybersecurity", UNIDIR, 2021, https://unidir.org/publication/gender-approaches-to-cybersecurity/.

188 Katharine Millar and Verónica Ferrari, "A Novel Approach to the 11 UN Norms for Responsible State Behaviour in Cyberspace: Guidelines for Gendered Implementation", UNIDIR, 2025, https://unidir.org/publication/a-novel-approach-to-the-11-un-norms-for-responsible-state-behaviour-in-cyberspace-guidelines-for-gendered-implementation/.

189 See UNIDIR, "UNIDIR Delivers Bilateral Cyber Capacity-Building and Policy Training in Thailand", 23 May 2025, https://unidir.org/unidir-delivers-bilateral-cyber-capacity-building-and-policy-training-in-thailand/; UNIDIR, "UNIDIR and Lao PDR Partner to Boost Cybersecurity Capacity", 4 August 2025, https://unidir.org/unidir-and-lao-pdr-partner-to-boost-cybersecurity-capacity/; UNIDIR, "UNIDIR Scales Up Cyber Resilience in Indonesia", 17 October 2025, https://unidir.org/unidir-scales-up-cyber-resilience-in-indonesia/; and UNIDIR, "UNIDIR Drives Cyber Resilience and Security in the Philippines", 26 November 2025, https://unidir.org/unidir-drives-cyber-resilience-and-security-in-the-philippines/.

Good Practices: Research to guide implementation of gender-responsive CCB

Some organizations have specifically worked on guides and handbooks to effectively integrate gender into CCB, including the following:

- **UN Women** contextualized this conversation for South-East Asia and published a **Facilitator's Manual** on cybersecurity threats, vulnerabilities, and resilience among women human rights defenders and civil society in the region.[190] The manual is a guide for facilitators and organizers in planning, preparing for, and conducting training sessions aimed at building cybersecurity capacity and resilience.
- The **GFCE** published a **Concept Note** on mainstreaming gender in CCB, including an agenda for gender-responsive CCB and specific activities to achieve it.[191]
- The **Association for Progressive Communications** developed a **Policy Explainer** on a gender-sensitive approach to CCB, which underlines that failing to design gender-sensitive CCB programmes could result in marginalisation of those who are already at risk.[192]

D. Integrating Gender-Responsive CCB in Relevant Governance Frameworks

CCB initiatives are not an isolated or standalone avenue for mainstreaming gender, and should be rooted in an ecosystem of experts working on the technology, processes, and governance frameworks. Participants drew several links between CCB programmes and the integration of gendered perspectives in cross-cutting national and industry considerations.

Key Recommendations

- Apart from cybersecurity frameworks, **link gender-responsive CCB with broader policies, processes and practices** on gender, security, and technology. This integration helps to **break silos among communities working on similar agendas** but within different policy processes or domains.
- Integrate gender perspectives into **CCB initiatives led by industry and international law actors**, including through practical exercises to illustrate real-world implications.

190 UN Women and UN University Institute in Macau, "Facilitators' Manual: Cybersecurity Threats, Vulnerabilities and Resilience Among Women Human Rights Defenders and Civil Society in South-East Asia", 2024, https://asiapacific.unwomen.org/en/digital-library/publications/2024/07/facilitators-manual-cybersecurity-threats-vulnerabilities-and-resilience-among-women-human-rights-defenders-and-civil-society-in-south-east-asia.

191 Global Forum on Cyber Expertise, "Mainstreaming Gender in Cyber Capacity Building", 2022, https://thegfce.org/wp-content/uploads/GFCE-Concept-Note-on-Mainstreaming-Gender-In-Cyber-Capacity-Building-2.pdf.

192 Association for Progressive Communications, "APC Policy Explainer: What Is a Gender-Sensitive Approach to Cyber Capacity Building?", 30 June 2023, https://www.apc.org/en/pubs/apc-policy-explainer-what-gender-sensitive-approach-cyber-capacity-building.

Several former WiC Fellows who participated in the workshops mentioned that the Fellowship empowered them to lead national processes on cybersecurity, including mainstreaming gender into different national policies, normative frameworks, and national capacity-building initiatives. However, the political will of governments is the key catalyst here. Some States have already taken steps to advance CCB programmes for women, such as **Mauritius** which convened a capacity-building workshop for policymakers and technical staff of various national ministries focused on digital upskilling for women and girls in 2024.[193]

The **ICT4Peace Foundation** and the **Global Network of Women Peacebuilders (GNWP)** published a report titled *Gendering Cybersecurity through Women, Peace and Security*, which provides ideas on mainstreaming gender into CCB programmes by maintaining the WPS Agenda as a foundation,[194] and thus breaking the policy silos between cybersecurity and gender-responsive frameworks. Collaborating with industry audiences may also be of specific interest when States consider more technical or hands-on CCB approaches. For instance, **North Macedonia** engaged in upskilling women cyber professionals through corporate partnerships and mentoring programmes[195] with the **Women4Cyber Foundation**.[196] The cybersecurity industry also runs CCB initiatives which focus on diversity in the field. An example highlighted in the workshops includes the **Women of FIRST** special interest group (SIG) under the auspices of the **Forum of Incident Response and Security Teams' (FIRST**). Women in FIRST is a gender-diverse group of practitioners supporting the increased participation of women in cybersecurity, through mentorship, networking, and knowledge-sharing.[197]

E. Considering Intersectionality and a Human-Centred Approach

While the CCB programmes discussed during the workshop were gender-responsive, the participants brought up the importance of framing them as essentially a human-centred approach aimed at fostering intersectional communities of practice. Apart from keeping programmes inclusive by design, a human-centred approach ensures that the momentum of activities around CCB is maintained regardless of the surrounding political, social, and security context, and also builds sustainable alliances and networks through various programmes.

Key Recommendations

- **Integrate intersectional considerations in the design, development, and delivery** of CCB programmes, including accounting for differentiated impacts across gender, age, race, ability, linguistic differences, and other contextually relevant factors.

193 Government Information Service of Mauritius, "Capacity Building Workshop Focuses on Digital Upskilling for Women and Girls in Africa", 6 May 2024, https://www.govmu.org/EN/newsgov/SitePages/Capacity-building-workshop-focuses-on-digital-upskilling-for-women-and-girls-in-Africa.aspx.

194 Julia-Silvana Hofstetter and Panthea Pourmalek, "Gendering Cybersecurity through Women, Peace and Security: Gender and Human Rights in National-level Approaches to Cybersecurity", 2023, https://ict4peace.org/wp-content/uploads/2023/03/Gendering-Cybersecurity-through-WPS-Final-Report_March-2023.pdf.

195 Women4Cyber, https://women4cyber.eu/.

196 Women4Cyber, https://women4cyber.mk/, and a participant in UNIDIR-Stimson Center workshops on gender mainstreaming in cybersecurity.

197 See Forum of Incident Response and Security Teams, "Women of FIRST SIG", https://www.first.org/global/sigs/wof/.

- **Establish networking as a core pillar of gender-responsive capacity-building**, including structured opportunities for peer exchange, mentorship, and engagement with broader stakeholder communities. Strong networks created through capacity-building programmes were highlighted by participants, who noted they help to further strengthen and amplify gender mainstreaming efforts

Providing opportunities for networking is essential to ensure lasting impacts of training programmes. The **GFCE** pursued this by establishing the **Women in Cyber Capacity Building Network (WiCCB)**, an informal network which brings together women cybersecurity professionals and seeks to amplify the impact of different gender-responsive cybersecurity efforts undertaken by GFCE.[198] A subset of this network, the **Network of African Women in Cybersecurity** (NAWC),[199] includes a group of experienced women professionals from the African region who provide expert advice and technical guidance at the national, regional, and continental levels to close gaps in gender-responsive cybersecurity planning, development, and implementation in Africa.[200]

The cascading effects of networking are not accidental, and can and should be designed into CCB programmes. For instance, the **Organization of American States (OAS)**, through its **Cynder Project**,[201] coordinates the **Women in Cybersecurity Empowerment (WiCE) Network**[202] in Latin America, which aims to amplify women's narratives and lived experiences in cybersecurity and raise awareness as a strategy to introduce structural change in cybersecurity cultures and practices. In Africa, Central Asia, and Europe, the **ITU** delivers a CCB programme titled **Her CyberTracks**[203] to women professionals from different communities of practice under three tracks — Policy & D, Incident Response, and Criminal Justice – with a specific focus on fostering networking opportunities across domains and regions.

198 Global Forum on Cyber Expertise, "Women in Cyber Capacity Building Network: Workplan", 16 January 2024, https://thegfce.org/tools/women-in-cyber-capacity-building-network-workplan/.

199 Global Forum on Cyber Expertise, "Africa Agenda for Cyber Capacity Building", https://gc3b.org/wp-content/uploads/2023/12/Africa-Agenda-Final-Final_Dec-.pdf.

200 "The Network of African Women in Cybersecurity (NAWC)", https://cybilportal.org/actors/the-network-of-african-women-in-cybersecurity-nawc/.

201 Organization of American States, "Cynder Project: Addressing the Gender Gap in the Cybersecurity Agenda of the Americas and the Caribbean", https://www.oas.org/ext/en/security/cynder-project.

202 Organization of American States, Women in Cybersecurity, https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=1404&lang=1.

203 ITU, "Her CyberTracks", https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Skills-Development/Her-CyberTracks.aspx.

Conclusion and Cross-Cutting Recommendations

This Compendium has aimed to systematize good practices and useful examples of gender mainstreaming into cybersecurity understandings, interpretations, measures, policy and institutional frameworks and awareness-raising and capacity-building initiatives. The aim is to provide States and other relevant stakeholders working on cybersecurity with useful tools to develop, implement, and operationalize an inclusive and gender-responsive cybersecurity architecture in line with the UN framework for responsible State behaviour in cyberspace towards the end of a secure, stable, and resilient digital future.

At the beginning of each workshop, participants addressed the same overarching question: how can we ensure that gender is not treated as a performative checkbox or a siloed issue, but rather integrated meaningfully across all aspects of cybersecurity? The word cloud below represents the most common answers and was compiled through an interactive activity with participants during the workshops. These answers not only encompass the breadth of the discussion across the workshops and this Compendium but also distil the experience of a broad range of experts into a bite-sized summary of the potential areas of future action to mainstream gender into cybersecurity.

The results are clear: representation and leadership of women in cybersecurity processes and its governance matters, but this is also multifaceted and contextual, as well as supported by a number of other recommendations mentioned in the cloud. Awareness and education were seen as key to understanding what cyber-risks and harms entail to individuals, groups, and communities in practice and support the implementation of legal and policy frameworks in a gender-sensitive and cross-cutting manner. Integration of gender considerations can be done through the life cycle of cybersecurity policies, from the initial assessment to their monitoring and evaluation. Finally, promoting gender-responsive CCB efforts, strong mentorship programmes, and sustained institutional support transform individual empowerment into systemic impact.

Drawing on the good practices gathered throughout the Compendium process, the following **cross-cutting recommendations** can provide a framework for communities of practice to institutionalize gender considerations in cybersecurity.

Cross-Cutting Recommendations

- Prioritize **evidence-based interpretations, policies and measures** through:
- **promotion of dedicated context-specific research** on the threat landscape to understand differentiated effects of cyber threats..;
- **collection and systematization of gender-disaggregated data** to understand specific ways different populations experience cyber threats and incidents and the severity of gendered harms, by tracking diversity within the cybersecurity workforce and the broader gender digital divide, to inform substantive changes on cyber threat modelling and risk assessments, and to establish baselines for policy development and implementation of national commitments; and
- **integration of gender-specific indicators** throughout the monitoring and evaluation schemes of cybersecurity frameworks to measure their success and room for improvement and to provide a technical baseline for gender mainstreaming.
- Adopt a **human-centred, intersectional, and contextualized approach** to cybersecurity, recognizing and responding to differentiated vulnerabilities faced by various groups, including on the basis of gender.
- Promote **mentorship and sustained capacity-building initiatives** to empower people of all gender expressions to engage equally and meaningfully in cybersecurity-related matters, from law interpretation and policy development to threat modelling and cybersecurity governance and diplomacy.
- Strengthen **awareness-raising, education, and training** of policymakers and national authorities in charge of implementing measures, standards, and commitments, including the judiciary, law enforcement, and armed forces, to foster a gender-sensitive understanding of and response to cyber harms.

- Promote **diversity in teams and the meaningful participation and leadership** of women and gender-diverse individuals at the different stages of the cybersecurity ecosystem, including technical, diplomatic, legal, and policymaking roles.
- Provide and secure **consistent funding** for gender mainstreaming initiatives to ensure long-term and systemic impact.
- Implement inclusive **consultations with a wide range of stakeholders**, to understand and consider diverse perspectives in gender mainstreaming in legal, policy, and institutional frameworks.
- **Institutionalize cross-sectoral coordination and policy coherence**. Bridge gaps across communities of practice to promote substantive engagement among cybersecurity practitioners, policy and legal experts, and gender and digital rights experts, in order to foster the development of well-informed and consistent standards, interpretative approaches, and frameworks.
- **Bridge the online–offline gap** to integrate cyber and digital issues into broader gender-related frameworks, such as international human rights law and the WPS Agenda, and ensure that obligations and commitments on equality, protection, participation, and prevention are also applied in the digital realm.

Toolbox of Resources

- Association for Progressive Communications, **APC Framework for Developing Gender-Responsive Cybersecurity Policy: Assessment Tool**
- Association for Progressive Communications, **Policy Explainer and Assessment Tool on Gender-Sensitive Approach to Cyber Capacity Building**
- Centre for Feminist Foreign Policy, **Feminist Perspectives on the Militarisation of Cyberspace**
- Chatham House, **Integrating Gender in Cybercrime Capacity-Building: A Toolkit**
- Committee on the Elimination of Discrimination against Women, **General Recommendation No. 35**
- Council of Europe, **Gender Mainstreaming in Thematic Areas: Gender Equality and Cybercrime / Cyberviolence**
- Cyber4Dev, **A Gender Mainstreaming Toolkit**
- European Institute for Gender Equality, **Gender Impact Assessment: Gender Mainstreaming Toolkit**
- FIRST (Forum of Incident Response and Security Teams), **Women of FIRST special interest group (SIG)**
- Global Forum on Cyber Expertise, **Mainstreaming Gender in Cyber Capacity Building**
- Global Partners Digital, **GPD Unveils New Guide to Fostering Inclusive Cyber Norm Processes**
- Human Rights Council, **The Promotion, Protection and Enjoyment of Human Rights on the Internet**, A/HRC/RES/47/16
- Human Rights Council, **The Right to Privacy in the Digital Age,** A/HRC/RES/54/21
- ICRC, **Gendered Impacts of Armed Conflict: Exploring Implications for IHL Governing the Conduct of Hostilities**
- ICT4Peace, **Women's Peace and Security in the Digital Age: An Emerging Agenda for Action**
- ICT4Peace and GNWP, **Gendering Cybersecurity through Women, Peace and Security: Gender and Human Rights in National-level Approaches to Cybersecurity**
- International Telecommunication Union, **Créer des Communautés Numériques Inclusives**
- International Telecommunication Union, **Handbook on Mainstreaming Gender in Digital Policies**
- International Telecommunication Union, **Her CyberTracks Programme**
- International Telecommunication Union, The World Bank, et al., **Guide to Developing a National Cybersecurity Strategy, 3rd Edition – Strategic Engagement in Cybersecurity**
- Organization of American States, **Cybersecurity Capacity and Talent Development Program.**
- Organization of American States, **Cynder Project**
- Organization of American States, Inter-American Commission of Women, and Follow-up Mechanism to the Belém do Pará Convention, **Principales Herramientas Conceptuales y Jurídicas para Prevenir, Sancionar y Erradicar la Violencia de Género contra las Mujeres Facilitada por las Tecnologías**

- Organisation for Economic Co-operation and Development, **Toolkit for Mainstreaming and Implementing Gender Equality 2023**
- Stimson Center, **Gendered Disinformation: A National Security Threat?**
- UN Women, **Facilitator's Manual on Cybersecurity and Women Human Rights Defenders**
- UN Women, **Handbook on Gender Mainstreaming for Gender Equality Results**
- United Nations Costa Rica, **Guía de Acción para Enfrentar la Violencia Digital contra las Mujeres en Política**
- United Nations Educational, Scientific and Cultural Organization and EQUALS Skills Coalition, **Je Rougirais si Je Pouvais : Réduire la Fracture Numérique entre les Genres par l'Éducation**
- United Nations Office to the African Union, **Note d'Orientation: L'Inclusion Numérique dans l'Agenda Femmes, Paix et Sécurité en Afrique**
- United Nations Population Fund, **Hacer Que Todos los Espacios Sean Seguros**
- United Nations Population Fund, **Resource Compendium on Technology-Facilitated Gender-Based Violence**
- UNIDIR, **Cyber Policy Portal**
- UNIDIR, **Gender Approaches to Cybersecurity, UNIDIR**
- UNIDIR, **Women in AI Fellowship**
- UNIDIR and Organization of American States, **A Novel Approach to the 11 UN Norms for Responsible State Behaviour in Cyberspace: Guidelines for Gendered Implementation**
- Women's International League for Peace and Freedom and Association for Progressive Communications, **Why Gender Matters in International Cyber Security**

Annex: Workshop Questions

Overarching Questions

- How do we ensure that gender is not treated as a performative checkbox or a siloed issue, but integrated meaningfully across all aspects of cybersecurity?
- In your area of practice, can you highlight one approach that has been successful in mainstreaming gender in cybersecurity? If none exist, can you mention an approach or method that you think could effectively help with mainstreaming efforts?

Guiding Questions for the Workshop on Threats and Impacts of ICTs on Gender

- How do cyber threats differently affect women, men, girls, boys, and gender minorities? Are the effects different depending on the type of cyber threat/activity?
- What existing strategies or initiatives have been effective in addressing gender-differentiated and gender-based cyber threats? What is missing in these and how can we fill that gap?
- What types of data and research are needed to better understand and address the gendered impacts of cyber threats? What are good practices for collecting gender-disaggregated data on ICT use and cyber threats?
- In what ways can the use of ICTs promote gender equality?

Guiding Questions for the Workshop on International Law, Norms, and Commitments in Cyberspace in the Context of Gender

- How do existing international frameworks (e.g., the Charter of the United Nations, international humanitarian law, international human rights law, the Convention on the Elimination of All Forms of Discrimination against Women) address the gendered impacts of cyber threats? What are the gaps?
- How can national policies address gender equality and cybersecurity and align with international commitments on these?
- Are there examples of good practices from national or regional initiatives that promote gender-sensitive interpretation and implementation of the 11 norms of responsible State behaviour?
- In what ways do cyber threats impact States' ability to meet their international legal obligations on gender equality and to prevent gender discrimination? How can international law be better leveraged to protect against gender-based and gender-differentiated cyber threats?
- How could gender be mainstreamed in future UN discussions on ICT security through the Global Mechanism?

Guiding Questions for the Workshop on Mainstreaming Gender into National Cyber Policies and Practices

- In your national or regional experience, what are the most effective methods for integrating gender considerations throughout the entire life cycle of digital and cybersecurity policy development, from initial assessment through implementation and evaluation? Methods can vary at different stages of the life cycle. What obstacles have you encountered?
- What are examples of successful gender mainstreaming in other policy areas that could be adapted for cybersecurity? What indicators or benchmarks can help to track progress on integrating gender in national cybersecurity policies?
- How can policy and technical discussions on evolving cyber threats better include diverse voices? What role can multi-stakeholder collaboration play in developing inclusive and gender-responsive cybersecurity strategies?
- How can the Women, Peace and Security (WPS) Agenda prevent, reduce, or address technology-facilitated gender-based violence? What are some avenues to improve engagement between national cybersecurity frameworks and the WPS Agenda?

Guiding Questions for the Workshop on Gender-Responsive Cyber Capacity Building

- In what ways can gender-responsive capacity-building strengthen national, regional, and global cybersecurity resilience? How can training programmes be designed to address this?
- What are key elements of a gender-responsive approach to cyber capacity-building? What good practices or models of gender-responsive capacity-building exist at national, regional, or international levels?
- What training, tools, or institutional support are needed to build capacity for gender-sensitive cybersecurity governance?
- What indicators or frameworks can help to assess whether capacity-building initiatives are gender responsive?

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

Palais de Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG