APC

THE MISSING LINK



Cybersecurity and technology-facilitated gender-based violence in the Women, Peace and Security agenda

HOW NATIONAL ACTION PLANS ADDRESS (AND OVERLOOK) DIGITAL THREATS

The missing link: Cybersecurity and technology-facilitated gender-based violence in the Women, Peace and Security agenda

How national action plans address (and overlook) digital threats

Author: Kristine Baekgaard[1]

Coordination and review: Verónica Ferrari (APC)

Proofreading: Laura Pérez Carrara

Layout proofreading: Lori Nordstrom (APC)

Design and layout: Constanza Figueroa Bustos

Published by the Association for Progressive Communications (APC), 2025

ISBN 978-92-95113-77-0
APC-202510-SEJ-R-EN-DIGITAL-367

Creative Commons Attribution 4.0 International (CC BY 4.0)
https://creativecommons.org/licenses/by/4.0/

1 Kristine Baekgaard (she/her) is a doctoral student in International Relations at the London School of Economics. Her research focuses on the intersections of technology, gender and security, with a specific focus on the intersection of Women, Peace and Security and technology-facilitated gender-based violence.

Acknowledgements

APC would like to thank Dr. Katharine Millar, associate professor of International Relations at the London School of Economics and Political Science, for her valuable feedback on this report. We are additionally grateful for her collaboration in identifying national action plans and generously sharing her database, which contributed greatly to the research process.

We would also like to thank Cailin Crockett, former Director, White House National Security Council/Senior Advisor, White House Gender Policy Council, 2021-2024, and Tazreen Hussain, former Women, Peace and Security Policy Advisor, USAID, for their insights and commentary on integrating technology-facilitated gender-based violence (TFGBV) into the United States National Action Plan.

We are finally grateful to the experts who generously shared their time, insights and experience during the workshop that informed this report.

Table of contents

Executive summary 5

Key findings 6

Key recommendations 7

Key concepts 10

Notable resolutions, frameworks and agendas 14

Methodology 20

Literature review 23

Analysis of NAPs and RAPs 32

Case study: Colombia 37

Case study: ASEAN 41

Getting TFGBV into the US National Action Plan 43

Conclusion and recommendations 44

Executive summary

October 2025 marks the 25th anniversary of United Nations Security Council Resolution 1325, which launched the Women, Peace and Security (WPS) agenda.[2] This milestone offers a critical opportunity for the international community to reflect on the profound changes in the peace and security landscape over the past two decades, including the rapid development and expansion of technology. When the WPS agenda was first adopted in 2000, the digital revolution was still in its early stages. Today, technology and digital spaces are deeply embedded in both our personal lives and in the practices of conflict and peace.

Extensive research has explored how technology can advance the goals of the WPS agenda, creating unprecedented opportunities for the participation,[3] empowerment[4] and peacebuilding efforts,[5] of women and gender-diverse people.[6] Yet, alongside these opportunities, the rapid spread of digital tools has also created new avenues for violence and marginalisation,[7] presenting new obstacles to the WPS agenda. Despite increasing calls from activists and an expanding body of research documenting the intersections of WPS, cybersecurity and technology-facilitated gender-based violence (TFGBV), these issues remain insufficiently integrated into mainstream WPS analysis and implementation. This gap is not merely an oversight, but a fundamental misalignment between the evolving nature of the security threats women and gender-diverse people face and the frameworks meant to address them. WPS national action plans (NAPs), in particular, have shown limited engagement with cybersecurity concerns.

This report explores the intersections of WPS, cybersecurity and TFGBV through both analytical and practical lenses. It first reviews existing research, then assesses how WPS NAPs address, or fail to address, emerging digital challenges. From this analysis, it identifies opportunities to strengthen policy coherence and improve implementation. The report concludes with concrete recommendations for WPS actors, digital rights advocates and private sector stakeholders to bridge these gaps and advance a more inclusive, effective response to contemporary security challenges.

2 https://www.un.org/womenwatch/osagi/wps/

3 Harris, A. (2008). Young women, late modern politics, and the participatory possibilities of online cultures. *Journal of Youth Studies, 11*(5), 481-495. https://doi.org/10.1080/13676260802282950

4 ShareAmerica. (2023, 27 March). How technology can strengthen democracy. https://archive-share.america.gov/how-technology-can-strengthen-democracy/index.html

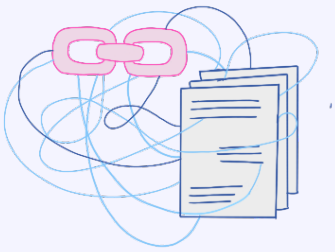
5 Tetteh, H. (2023). Horn of Africa: Using Digital Technologies to Advance Women, Peace and Security Agenda. *Africa Renewal April 2023*.

6 McInroy, L. B., Craig, S. L., & Leung, V. W. Y. (2019). Platforms and Patterns for Practice: LGBTQ+ Youths' Use of Information and Communication Technologies. *Child and Adolescent Social Work Journal, 36*, 507-520. https://doi.org/10.1007/s10560-018-0577-x

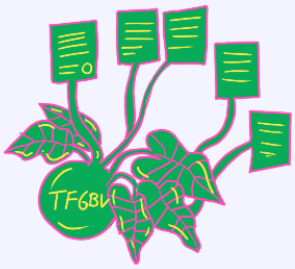
7 Baekgaard, K. (2024). *Technology-Facilitated Gender-Based Violence: An Emerging Issue in Women, Peace and Security. Research Report.* Georgetown Institute for Women, Peace and Security. https://giwps.georgetown.edu/wp-content/uploads/2024/06/Technology-Facilitated-Gender-Based-Violence.pdf

Key findings

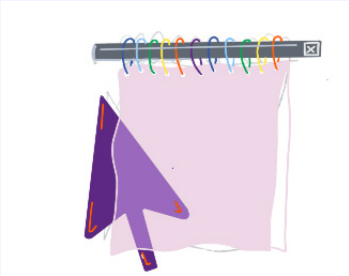
The following key findings summarise patterns, gaps and promising practices identified through a review of 37 national and regional action plans, highlighting how states are beginning to integrate cybersecurity and TFGBV within WPS-related commitments.



Engagement remains limited: The majority of NAPs analysed reference cyber-related issues only minimally, if at all, with just eight plans demonstrating what could be considered significant and cross-pillar engagement.



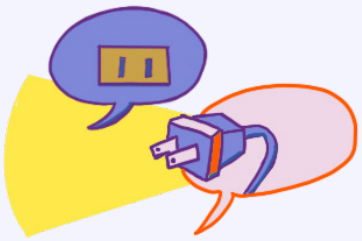
Digital gender-based violence is the most common entry point: Most NAPs that do reference cybersecurity do so in relation to online forms of gender-based violence, though the depth of analysis and proposed responses vary widely.



Few plans engage with the full WPS agenda: Only a small subset of NAPs meaningfully connect cyber issues to the three pillars of participation, protection and prevention, while the fourth pillar, relief and recovery, remains almost entirely absent.



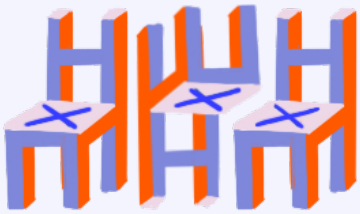
Participation gaps are beginning to be addressed: A growing number of NAPs acknowledge the importance of women's inclusion in cybersecurity policy and digital governance, though implementation strategies often remain underdeveloped.



NAPs are often disconnected from broader security strategies: Most plans fail to link WPS-related cyber concerns to national cybersecurity strategies, disinformation response efforts or early warning systems.



Digital rights frameworks are largely missing: Most NAPs, even those that explicitly address gender and cybersecurity, do not reference existing digital rights instruments or commitments, representing a major area for future alignment and policy coherence.



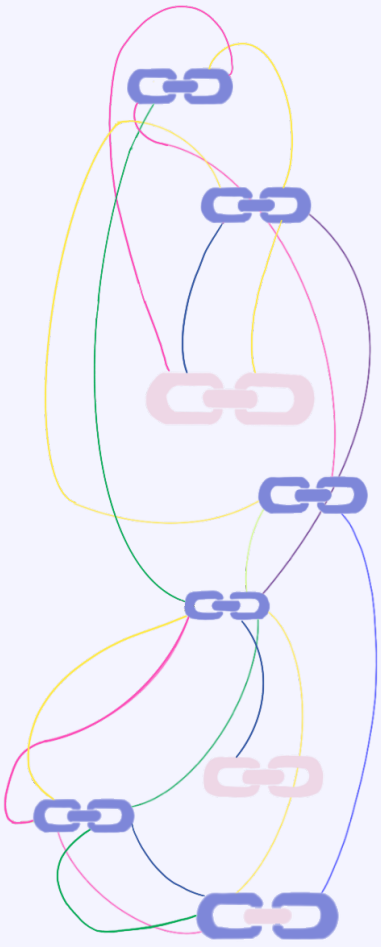
Technology companies and the private sector broadly are absent: Despite the central role that the private sector plays in the facilitation and amplification of digital violence, it is not engaged in any NAPs.

Key recommendations

To respond effectively to the rising digital dimensions of insecurity, violence and exclusion, this report outlines targeted recommendations for key stakeholder groups across the peace, security and technology ecosystems.

Recommendations for WPS actors

The WPS agenda must evolve to meet digital-era realities, with cyber threats now central to gendered insecurity.



Multilateral WPS actors

- Convene cross-sector dialogues between WPS experts and digital rights experts to improve mutual literacy.
- Use WPS mandates to advocate for gender-responsive digital laws and accountability mechanisms.
- Promote gender-responsive cybersecurity practices and policy through regional WPS mechanisms.
- Bridge the gap between WPS and digital rights frameworks.
- Support perpetrator-focused research and programming on TFGBV and digital violence.

National governments developing or implementing NAPs

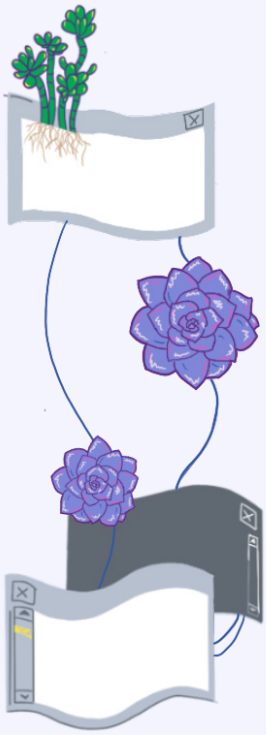
- Conduct inclusive, intersectional consultations with affected and expert communities.
- Include measurable and resourced cyber commitments in WPS NAPs.
- Expand definitions of security to include domestic digital harms.
- Institutionalise collaboration between WPS and digital policy ministries.
- Promote diversity and inclusion across cybersecurity, technology and security sectors.
- Fund intersectional research on digital spaces.

Civil society and peacebuilders

- Continue to document and disseminate evidence on digital harms and effective responses.
- Build cross-sector partnerships between peacebuilders and tech experts.
- Amplify marginalised voices in global WPS and digital policy forums.
- Develop and distribute localised, practical safety resources.

Recommendations for digital rights actors

Digital rights and cybersecurity actors must treat WPS as core to peace and digital security.



International cybersecurity and digital rights bodies

- Integrate WPS perspectives into global digital governance forums.
- Include WPS actors, especially from the Global South, in cybersecurity policy making.
- Map overlaps between NAPs and cyber strategies to align approaches.
- Advocate for the inclusion of gender and technology-facilitated gender-based violence (TFGBV) issues in cyber policy dialogues.

National governments (cybersecurity, ICT and digital ministries)

- Embed gender considerations across all digital policies and cybersecurity strategies.
- Partner with WPS actors to coordinate on TFGBV and digital harms.
- Hold tech platforms accountable for preventing and addressing online abuse.
- Use WPS principles to guide digital regulation and platform oversight.

Civil society organisations

- Co-create multilingual terminology frameworks bridging WPS and cyber fields.
- Facilitate local-global knowledge sharing between peacebuilders and digital rights actors.

Recommendations for technology companies

Tech companies must be accountable partners in making digital spaces safer for all.



- Invest in gender diversity across teams, especially in cybersecurity and AI.
- Design safety features and content moderation tools with a gender lens.
- Ensure accessible, multilingual (including local and vernacular languages) and effective reporting and redress systems.
- Collaborate with WPS and civil society actors to co-create inclusive solutions.
- Fund research and innovation on gender-responsive digital safety and TFGBV.

Key concepts

Because terms such as *cybersecurity, digital rights* and *technology-facilitated gender-based violence (TFGBV)* are used differently across policy, advocacy and academic spaces, it is important to clarify how they are understood here. Establishing a shared language does not mean imposing a single "correct" definition, but rather ensuring clarity for the purposes of this analysis. To that end, the following definitions outline how these terms are used throughout this report.

Gender

Gender refers to the social and cultural processes that shape how people are perceived, expected to behave and experience rights, resources and power. It is not fixed or binary but constructed in relation to other aspects of identity such as sexuality, race, class, ability, age, religion and political context. Applying a gender lens means recognising these intersections, addressing structural inequalities and ensuring that different women, men and gender-diverse people are meaningfully included in shaping digital technologies, policies and spaces.[8]

Gender-responsive policy making

Gender-responsive policy-making practice extends beyond addressing inequalities within specific policies; it proactively designs policies intended to advance gender equality.[9]

Intersectionality

An intersectional perspective recognises that people experience multiple, interconnected forms of oppression, including based on gender, race, religion and class, which together shape complex social, economic and other hierarchies. Individuals are rarely affected by a single form of oppression in isolation.[10]

Women, Peace and Security agenda

The Women, Peace and Security (WPS) agenda refers to a global framework that was first formalised through United Nations Security Council Resolution 1325 (UNSCR1325)

8 UN Free & Equal. (2025). *Know the Facts. Definitions.* https://www.unfe.org/know-the-facts/definitions

9 Millar, K., & Ferrari, V. (2025). *A Novel Approach to the 11 UN Norms for Responsible State Behaviour in Cyberspace: Guidelines for Gendered Implementation.* UNIDIR & OAS/CICTE. https://unidir.org/wp-content/uploads/2025/05/UNIDIR_Novel_Approach_11_UN_Norms_Responsible_State_Behaviour_Cyberspace_Guidelines_Gendered_Implementation.pdf

10 Association for Progressive Communications. (2023). *A Framework for Developing Gender-Responsive Cybersecurity Policy: Assessment Tool.* https://www.apc.org/sites/default/files/apcgendercyber-assessmenttool.pdf

in October 2000.[11] The resolution recognised women's unique and diverse experiences of and contributions to conflict and peace[12] and the framework is currently comprised of 10 resolutions, structured around four pillars:[13]

1. Women's equal and meaningful **participation** in decision making in local, national, regional and international institutions and in peace processes.
2. The **protection** of women's and girls' human rights and from sexual and gender-based violence (GBV).
3. **Prevention of violence against women and of conflict more broadly**.
4. The inclusion of provisions for women's specific needs in **relief and recovery** efforts.

Various actors, including governments, civil society organisations and international organisations, each use different mechanisms, policies and strategies to implement the WPS agenda with the shared goal of achieving gender equality and sustainable peace.

While UNSCR 1325 and subsequent resolutions stick to the binary language of "women and men", some actors interpret the agenda more broadly and include LGBTQI+ and non-binary people, though this is not widely implemented across NAPs.

National action plans

National action plans (NAPs) are the primary implementation mechanism at the state-level for the WPS agenda. NAPs are an overview of a given state's priorities, strategies and concerns with regards to implementing WPS.[14] There are also some examples of regional action plans (RAPs), including from the Southern African Development Community (SADC) and the Economic Community of West African States (ECOWAS),[15] which aim to coordinate WPS efforts across multiple countries in a specific region.

Digital vs. online vs. cyber

The terms digital, online and cyber are sometimes used interchangeably, but they are distinct.

> *Digital* refers to anything that exists in binary form (images, text, music, software).[16] *Online* refers to anything that is connected to the internet. Everything

11 UN Women Moldova. (2025). *Fact Sheet: The Women, Peace and Security Agenda.* https://moldova.unwomen.org/en/digital-library/publications/2025/05/fact-sheet-the-women-peace-and-security-agenda

12 United Nations Department of Peace Operations. *Women, Peace and Security.* https://www.un.org/en/peace-and-security/page/women-peace-and-security

13 https://www.un.org/shestandsforpeace/content/four-pillars-united-nations-security-council-resolution-1325

14 Biddolph, C., & Shepherd, L. J. (2024). *WPS National Action Plans: Content Analysis and Data Visualisation, v4.* University of Sidney Centre for International Security Studies. https://www.wpsnaps.org/

15 https://www.un.org/shestandsforpeace/content/regional-action-plans-0

16 Manaher, S. (n/d). Digital vs Online: Deciding between Similar Terms. *The Content Authority.* https://thecontentauthority.com/blog/digital-vs-online

online is digital, but not everything digital is online.[17] *Cyber* is generally used as a prefix (*cyber*security, *cyber*crime, etc.) and indicates the involvement of computers or networks.[18]

Cybersecurity

Cybersecurity refers to the development of norms, protocols and technical protections to ensure the safety and integrity of infrastructures, networks, information and systems from external cyberattacks.[19]

Gender-based violence (GBV)

Gender-based violence is a term used to describe any harmful act perpetrated against a person based on socially ascribed gender differences between males and females. It includes acts causing physical, sexual or mental harm or suffering, or threats of such acts, and other deprivations of liberty.[20] Online and offline gender-based violence do not happen in vacuums separate from each other, as women's and gender-diverse people's lives online intersect frequently and in various complex ways with other areas of their lives, and violence in any one domain can often produce harm across other domains.[21] Recognising this continuity is crucial, as it means that effectively addressing digital violence requires more than just technical solutions; it demands confronting and dismantling the root causes of patriarchy and gender inequality.

Technology-facilitated gender-based violence (TFGBV)

Technology-facilitated gender-based violence (TFGBV) – such as cyberstalking, online harassment and doxxing – encompasses acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs), such as phones, the internet, social media platforms and email.[22] TFGBV has the same roots as other forms of gender-based violence and is part of the same continuum.[23]

Online gender-based violence (OGBV)

Online gender-based violence is the term that came before TFGBV and which is still used by some actors. It refers to gendered violence that specifically takes place

17 Ibid.

18 https://www.merriam-webster.com/dictionary/cyber

19 https://www.apc.org/en/glossary/cybersecurity

20 UNICEF Serbia. (2021). *Gender-Based Violence Information Pack. Strengthening Refugee and Migrant Children's Health Status in Southern and South-Eastern Europe.* https://www.unicef.org/serbia/en/media/16751/file

21 Association for Progressive Communications. (2023). *Feminist Principles of the Internet: Advocacy brief on violence.* https://genderit.org/FPI-paper-on-violence

22 https://www.apc.org/en/glossary/technology-facilitated-gender-based-violence

23 Association for Progressive Communications. (2023). Op. cit.

in online spaces.[24] While OGBV[25] is still used, TFGBV might be considered more comprehensive, as it also encapsulates violence that occurs through digital means (stalkerware, tracking devices, etc.), though not necessarily online.

24 Sanusi, T. (2021, 17 November). Online Gender-Based Violence: What You Need to Know. *Global Citizen*. https://www.globalcitizen.org/en/content/what-is-online-gender-based-violence-2/

25 Another term used by actors, including UN Women, in a policy context is online violence against women and girls (OVAWG).



Notable resolutions, frameworks and agendas[26]

The following resolutions, frameworks and agendas form the backbone of global efforts to address the issues of gender, peace and equality in digital spaces. Though they are not currently coordinated or explicitly aligned, they share similar core values of equality and security for all and may serve as a strong entry point for efforts to align the WPS and digital rights agendas.

Key Women, Peace and Security frameworks

Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)

1979

International treaty

A precursor to the WPS agenda, CEDAW is often described as an international bill of rights for women. It defines what constitutes discrimination against women and obligates states to address it in all areas, including legal, political, economic, social and cultural life.[27] CEDAW has developed a few general recommendations (GRs) with references to technology, including GRs 19, 35 and 40.[28]

The Beijing Declaration and Platform for Action

1995

Global agenda

The Beijing Declaration is considered to be the most progressive blueprint ever for advancing women's rights. It outlines a comprehensive global agenda for achieving gender equality and empowering women through strategic objectives and actions, and was designed with significant input from civil society, though it is not legally binding.[29]

26 The Association for Progressive Communications has created a more substantive outline of relevant tools, agendas and frameworks on gender and the digital space that cybersecurity policy makers may draw on specifically as part of their framework for developing gender-responsive cybersecurity policy. See: https://www.apc.org/en/pubs/framework-developing-gender-responsive-cybersecurity-policy

27 UN Women. (n/d). *Convention on the Elimination of All Forms of Discrimination against Women*. https://www.un.org/womenwatch/daw/cedaw/cedaw.htm

28 Office of the High Commissioner for Human Rights. (2024, 25 October). General Recommendation No. 40: Equal and Inclusive Representation of Women in Decision-Making Systems. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-recommendation-no-40-equal-and-inclusive

29 Association for Progressive Communications. (2022). *A framework for developing gender-responsive cybersecurity policy: Norms, standards and guidelines*. Association for Progressive Communications. https://www.apc.org/sites/default/files/gender-cybersecurity-policy-norms.pdf

United Nations Security Council Resolution 1325

2000

UN resolution

This resolution serves as the keystone for the Women, Peace and Security agenda, recognising the unique experiences and contributions of women in peace and security contexts. It calls for women's participation in peace negotiations, protection from gender-based violence during conflicts, prevention of conflict and the integration of gender-sensitive measures in relief and recovery efforts.[30]

Key frameworks addressing human rights and technology

United Nations General Assembly Resolution 53/70

1998

UN resolution

This resolution recognises the security implications of information and communications technologies (ICTs). It calls on member states to share views on threats to information security, encourages international cooperation to promote peaceful and secure ICT use and establishes the groundwork for future UN discussions on cybersecurity through a group of governmental experts.[31]

United Nations Human Rights Council Resolution 20/8

2012

UN resolution

This resolution affirms that fundamental rights, including freedom of speech, apply equally online and offline. It urges states to promote universal internet access and international cooperation to expand digital infrastructure, while also encouraging UN human rights mechanisms to integrate digital considerations into their work.[32]

30 Security Council. (2000). *Resolution 1325 (2000).* United Nations. https://docs.un.org/en/S/RES/1325(2000)

31 General Assembly. (1999). *Resolution 53/70. Developments in the Field of Information and Telecommunications in the Context of International Security.* United Nations. https://docs.un.org/en/A/RES/53/70

32 Human Rights Council. (2012). *Resolution 20/8. The promotion, protection and enjoyment of human rights on the Internet.* United Nations. https://documents.un.org/doc/resolution/gen/g12/153/25/pdf/g1215325.pdf

United Nations Framework for Responsible State Behaviour in Cyberspace

2016

UN resolution

The United Nations Framework for Responsible State Behaviour in Cyberspace sets out 11 voluntary norms and principles, grounded in international law, to guide states toward responsible conduct, conflict risk reduction and capacity building in cybersecurity.[33]

UN Group of Governmental Experts (GGE) Report on Advancing Responsible State Behaviour in Cyberspace

2021

UN expert report

The 2019-2021 GGE report reaffirms the applicability of international law and human rights in cyberspace and outlines 11 voluntary norms for responsible state behaviour. It emphasises the importance of the 11 norms of responsible state behaviour in cyberspace for human rights, with an emphasis on closing the gender digital divide.[34]

Key frameworks on gender and technology

Feminist Principles of the Internet

2014

Activist framework

The Feminist Principles of the Internet are a set of guidelines developed by activists to promote a digital world that is inclusive, equitable and free from online violence. They offer an iterative feminist framework to address technology and internet rights, centred around five clusters: access, movements, economy, expression and embodiment.[35]

33 General Assembly. (2015). *Resolution 70/237. Developments in the field of information and telecommunications in the context of international security.* United Nations. https://docs.un.org/en/A/res/70/237

34 General Assembly. (2021). *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.* United Nations. https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf

35 https://feministinternet.net/en/page/about

United Nations Human Rights Council Resolution 38/5

2018

UN resolution

This resolution affirms that all forms of violence against women and girls, including in digital spaces, must be addressed as human rights violations. It underscores member states' obligation to prevent, investigate and punish violence against women and girls in digital contexts and calls for integrating online safety into broader gender equality strategies.[36]

Report of the Special Rapporteur on the right to privacy (A/HRC/40/63): Privacy and technology from a gender perspective

2019

UN report

In this report, issues of privacy and gender are examined, focusing on privacy and personality, security and surveillance, gender and data. Among the recommendations, the report calls on states to adopt an intersectional approach that recognises the specific benefits, experiences and threats to the right to privacy according to gender, as well as overarching privacy and human rights principles.[37]

United Nations Human Rights Council Resolution 47/23

2021

UN resolution

This resolution addresses the intersection of human rights and emerging digital technologies, urging states to ensure that these technologies respect, protect and fulfil human rights. It calls for integrating human rights considerations, including gender equality, into the design, development and use of digital technologies.[38]

36 Human Rights Council. (2018). *Resolution 38/5. Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts.* United Nations. https://documents.un.org/doc/undoc/gen/g18/214/82/pdf/g1821482.pdf

37 Cannataci, J. (2019). *Report of the Special Rapporteur on the right to privacy.* United Nations. A/HRC/40/63. https://docs.un.org/en/A/HRC/40/63

38 Human Rights Council. (2021). *Resolution 47/23. New and emerging digital technologies and human rights.* United Nations. https://docs.un.org/en/A/HRC/RES/47/23

Report of the Special Rapporteur on freedom of opinion and expression (A/76/258): Gender justice and freedom of expression **2021** *UN report*	The report examines legal standards, state and corporate responsibilities and the challenges women face both online and offline. It emphasises that gender equality and freedom of expression are mutually reinforcing and essential for peace, democracy and sustainable development.[39]
CSW67 Agreed Conclusions **2023** *UN intergovernmental agreement*	Adopted at the 67th session of the Commission on the Status of Women (CSW67), these conclusions highlight the critical role of technology, innovation and digital education in advancing gender equality. They emphasise that online and offline gender-based violence are interconnected, urging stronger legal and policy frameworks to create safe, inclusive and accessible digital environments. This is the first UN intergovernmental agreement focused specifically on the intersection of gender and digital transformation.[40]
United Nations Human Rights Council Resolution 53/29 **2023** *UN resolution*	This resolution addresses the promotion, protection and enjoyment of human rights in the context of digital technologies. It emphasises the importance of closing the gender digital divide and ensuring that digital transformation is inclusive and rights respecting.[41]

39 Khan, I. (2021). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.* United Nations. https://docs.un.org/en/A/76/258

40 Commission on the Status of Women. (2023). *Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls. CSW67 Agreed Conclusions.* United Nations. https://www.unwomen.org/sites/default/files/2023-03/CSW67_Agreed%20Conclusions_Advance%20Unedited%20Version_20%20March%202023.pdf

41 Human Rights Council. (2023). *Resolution 53/29. New and emerging digital technologies and human rights.* United Nations. https://docs.un.org/en/A/HRC/RES/53/29

Report of the Special Rapporteur on freedom of opinion and expression (A/78/288): Gendered disinformation

2023

UN report

In this report, the negative impact of gendered disinformation, especially on women and gender diverse people, and its implications for freedom of expression are explored. The report clarifies that gendered disinformation is both a tactic to silence free expression and a threat to safety and health.[42]

Global Digital Compact

2024

UN-endorsed agreement

The Global Digital Compact (GDC) is an agreement endorsed by the United Nations that brings together all 193 member states and a wide range of stakeholders as part of the Pact for the Future, to promote a rights-based, inclusive digital future. It commits to: 1) closing the digital divide by ensuring universal, affordable and accessible connectivity; 2) safeguarding an open, secure and interoperable internet underpinned by human rights protections; and 3) establishing global frameworks for data governance and responsible AI.[43]

The GDC highlights gender equality and the participation of all women and girls in the digital space as core principles. It also calls for mainstreaming a gender perspective and addressing all forms of violence, including sexual and gender-based violence amplified by technology (principle d). Under objective 1 on connectivity, it commits to integrating a gender perspective into digital connectivity strategies.

42 Khan, I. (2023). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.* United Nations. https://docs.un.org/en/A/78/288

43 https://www.un.org/global-digital-compact/en

Methodology

This research was conducted in four phases: a literature review, a content analysis of national and regional action plans (NAPs and RAPs)[44] on Women, Peace and Security (WPS), case studies that provided in-depth insights to inform recommendations and a validation workshop. Together, these phases enabled the identification of key issues raised in the literature and an assessment of how they are addressed within the context of NAPs.

The first phase involved a comprehensive review of academic and policy literature at the intersection of WPS, cybersecurity and technology-facilitated gender-based violence (TFGBV). A structured search strategy produced a dataset of over 40 peer-reviewed articles, reports and policy briefs. These materials were thematically analysed to surface recurring issues and knowledge gaps, which then informed the analytical framework for the second phase.

In the second phase a systematic review of WPS NAPs and RAPs was conducted. Drawing on databases maintained by the WPS Focal Points Network[45] and the Women's International League for Peace and Freedom (WILPF),[46] 121 NAPs and RAPs were identified. For each country or region, the most recent available plan was selected to reflect the latest language and priorities, even if the plan was no longer active.[47] An initial screening was conducted using targeted keyword searches for "cyber", "digital", "technology" and "online".

One or more of these keywords were found in 52 plans. Of those, 11 were excluded for referencing digital tools solely in a programmatic context (e.g., online trainings) without discussing related risks or threats.[48] Another six were excluded for referencing "technology" only with respect to institutional actors (e.g., ministries of technology), rather than as thematic content.[49] This refinement yielded a final sample of 37 plans (34 NAPs and three RAPs), which were then subjected to in-depth qualitative analysis to assess how digital threats, cybersecurity and TFGBV are integrated into national and

44 For simplicity, the term RAP is used in this context to refer to any plan that engages with more than one country in a similar region.

45 The WPS Focal Points Network currently lists 106 national action plans and 10 regional action plans. https://wpsfocalpointsnetwork.org/wps-focal-points-members/

46 WILFP notes that 108 UN member states (56%) have adopted a national action plan under UNSCR 1325, although around 30% are currently outdated, having expired in 2022 or before. https://www.wilpf.org/external_posts/1325-national-action-plans-naps/

47 For the purpose of this study, the expiry date was not used to exclude NAPs from analysis, as they may still contain interesting insights on integrating WPS and cybersecurity. Additionally, given the time it takes for NAPs and RAPs to be re-written by states and organizations, some might still be under application, despite technical expiration.

48 These are the NAPs from Burkina Faso, Cyprus, Germany, Iraq, Jordan, Moldova, Palestine, Somalia, Spain, Tajikistan and Uganda.

49 These are the NAPs from Burundi, Mozambique, Nepal, Rwanda, South Sudan and Tunisia.

regional WPS policy frameworks. To complement this analysis, two case studies were selected for deeper examination: Colombia's National Action Plan and the Association of Southeast Asian Nations (ASEAN) Regional Plan of Action on WPS. These were chosen for their distinct contexts and strategic approaches, offering valuable insights into how national and regional mechanisms can differently shape, support and institutionalise cybersecurity within the WPS agenda.

In addition to the literature and policy analysis, two interviews were conducted with US government officials involved in the development of the United States National Action Plan (NAP) on WPS. These conversations provided further insights into how cybersecurity and TFGBV are being considered in national-level policy making and helped identify additional areas for alignment and improvement.

The fourth and final stage of the methodology was a validation workshop, conducted after the initial draft of the report was completed. The workshop brought together representatives from civil society, government and academia, with expertise spanning both the digital rights and WPS fields. Feedback from the session was incorporated into the report to strengthen its accuracy, relevance and resonance with the communities it seeks to engage.

Limitations

This report is subject to several limitations, as some areas necessarily fall outside its scope. The analysis is focused specifically on how TFGBV and cybersecurity are integrated into WPS NAPs. As such, it does not attempt to document the extensive and critical work that civil society organisations are undertaking at the intersections of WPS and TFGBV more broadly. That said, civil society perspectives remain central to this report and in shaping the analysis we have drawn extensively on CSO research, practice and consultations.

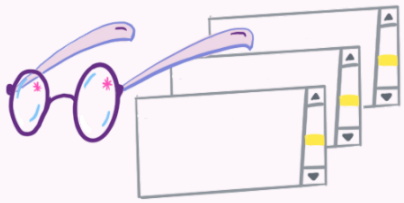
Second, the report does not address the political reality that many governments may have limited or even negative incentives to combat TFGBV and cybersecurity threats, particularly where digital repression or harassment serves the interests of authoritarian actors, which deeply shapes NAP creation and implementation.

Third, while it draws from the WPS framework, the report does not engage with broader debates about whether WPS is itself the most effective or inclusive lens through which to approach these issues, acknowledging its status as a highly contested norm.

Fourth, it does not fully explore the tension between state commitments to protect women and civilians and the continued pursuit of militarisation, including investment in military artificial intelligence (AI) and drones. This double standard complicates claims to a human security-oriented approach.

Finally, the report does not attempt to resolve the challenge of securing genuine state commitments. While NAPs and other frameworks often articulate ambitious promises, translating them into sustained action remains one of the most persistent obstacles for both WPS and cyber agendas.

Literature review



In recent years, scholars, practitioners and activists have begun exploring the intersection of the WPS agenda, cybersecurity and TFGBV. While this field is still emerging,[50] there is growing consensus among activists, academics and policy makers that cybersecurity frameworks must adopt a gender lens,[51] and conversely,[52] that the WPS Agenda must evolve to address cyber threats, including TFGBV,[53] which pose serious risks to the safety, agency and participation of women and gender-diverse people.[54] Beyond these two overarching points of consensus, researchers and practitioners have investigated a range of related issues, generating insights that can be broadly grouped into two categories: 1) those that outline the key issues linking WPS, cybersecurity and TFGBV; and 2) those that explore the challenges of aligning these agendas. While the body of research is expanding rapidly, and several areas remain underexplored, the link between these two issues is well established.[55]

There is also a growing body of literature that examines the gendered dimensions of cybersecurity more broadly. While a full review of this work is beyond the scope of this report, readers can refer to the literature review developed as part of the Association for Progressive Communication's (APC) *Framework for Developing Gender-Responsive Cybersecurity Policy* for a comprehensive overview.[56]

50 UN Women Asia and the Pacific. (2024). *Women, Peace and Digital (In)Security in South-East Asia – Reflections on Diverse Experiences in the Digital Sphere*. https://asiapacific.unwomen.org/sites/default/files/2024-10/un-women_digital_insecurity_2024-c.pdf

51 Mhajne, A., & Henshaw, A. (Eds). (2024). *Critical Perspectives on Cybersecurity: Feminist and Postcolonial Interventions*. Oxford University Press. https://doi.org/10.1093/oso/9780197695883.001.0001

52 Nair, T. (2022). The Women, Peace and Security Agenda in Digital Space. In G. Haciyakupoglu & Y. Wong (Eds.), *Gender and Security in Digital Space: Navigating Access, Harassment, and Disinformation*. Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003261605-3/women-peace-security-agenda-digital-space-tamara-nair

53 Whetstone, C., & Luna, K.C. (2024). A Call for Feminist Insights in Cybersecurity: Implementing United Nations Security Council Resolution 1325 on Women, Peace and Security in Cyberspace. In A. Mhajne & A. Henshaw (Eds). *Critical Perspectives on Cybersecurity: Feminist and Postcolonial Interventions*, 25-51. Oxford University Press. https://doi.org/10.1093/oso/9780197695883.003.0002

54 Fal-Dutra Santos, A., & Pourmalek, P. (2022). Preventing Violence in the Digital Age: Women Peacebuilders and Technology-Facilitated Gender-Based Violence. In M. Garrido V. (Ed.), *Mapping Online Gender-Based Violence*. University for Peace. https://upeace.org/wp-content/uploads/2024/04/Garrido-Mapping-Online-Gender-based-Violence.pdf#page=80

55 Millar, K., & Ferrari, V. (2025). Op. cit.

56 Association for Progressive Communications. (2022). Op. cit.

Key issues in WPS and cybersecurity

One of the first and most influential pieces of research on WPS and cybersecurity was a 2021 report by the United Nations Institute for Disarmament Research (UNIDIR) entitled *System Update: Towards a Women, Peace and Cybersecurity Agenda*.[57] In this report, the authors argue that the WPS agenda must evolve to address the specific threats women face in cyberspace, and they outline six priority areas to help "narrow the gap" between WPS and cybersecurity: 1) women's participation in cybersecurity negotiations; 2) cyberviolence against women and girls; 3) online harassment and women's participation in political processes; 4) gender and online radicalisation; 5) gendered impacts of cyber incidents; and 6) gender bias in digital technologies.[58] These six priorities remain highly relevant, with subsequent research reinforcing and elaborating on their significance. Notably, they also map closely onto the four pillars of the WPS agenda: participation, protection, prevention and relief and recovery.

Participation

In their report, Sharland et al. articulate three core dimensions of the WPS participation pillar in the context of cybersecurity.[59] The first – women's participation in cybersecurity negotiations – is one of the most frequently cited themes in the literature. UN Women emphasises that women are best positioned to articulate their cybersecurity needs and priorities,[60] a point that is further elaborated by APC and WILPF.[61] Others highlight women's general underrepresentation in the tech industry more broadly, calling for greater investment in women's leadership to prevent the replication of gender bias in digital systems. Ferron extends this argument to AI, asserting that women must play a central role in developing and training AI models,[62] given the unique threats they face.[63] Sharland et al.'s second and third priorities – cyberviolence against women and girls and online harassment's impact on political participation[64] – have been developed in the literature on TFGBV. In the context of WPS specifically, Baekgaard highlights the wide range of digital threats and the two primary ways such violence undermines participation. The first way is through direct attacks on women and gender-diverse people with influence (politicians, journalists and activists), which often lead

57 Sharland, L., Goussac, N., Currey, E., Feely, G., & O'Connor, S. (2021). *System Update: Towards a Women, Peace and Cybersecurity Agenda*. UNIDIR. https://doi.org/10.37559/GEN/2021/03

58 Ibid.

59 Ibid.

60 UN Women Asia and the Pacific. (2024). Op. cit.

61 Brown, D., & Pytlak, A. (2020). *Why Gender Matters in International Cyber Security*. Women's International League for Peace and Freedom & Association for Progressive Communications. https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf

62 Ferron, H. (2025). *WPS in the Digital Age: Investigating AI and International Cybersecurity Policy*. Research Network on Women, Peace and Security. https://www.rnwps.ca/policy-briefs/pb-1-holly-ferron

63 Capitol Technology University. (2024, 21 March). Artificial Intelligence and Its Unique Threat to Women. *Capitology Blog*. https://www.captechu.edu/blog/artificial-intelligence-and-its-unique-threat-women

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

to their withdrawal from public life.[65] Kakande et al. underscore the uniquely gendered nature of these attacks compared to those faced by men, reinforcing women's historical underrepresentation in political spaces.[66] The second way is through a chilling effect, whereby the threat of online violence deters people from participating in the first place.[67] Studying the Nepalese context specifically, Kayastha and Pokharel highlight how governments can contribute to this chilling effect by criminalising "obscene" speech, thereby curtailing marginalised communities' right to freedom of expression.[68] Focusing on peacebuilders specifically, Fal-Dutra Santos and Pourmalek find that TFGBV is nearly ubiquitous among women peacebuilders and is often deployed with the explicit intent of preventing their participation in peace and security processes.[69] The gender digital divide[70] also falls under WPS participation, particularly as ICTs are increasingly used in peacebuilding[71] to facilitate peace processes.[72] The lack of access to both hardware and platforms thus presents a challenge to women's full and equal participation.

Overall, the literature leaves us with several key issues as related to cybersecurity and the participation pillar:

- Underrepresentation of women in cybersecurity policy making and negotiations.
- Underrepresentation of women in digital industries, reinforcing gender bias in technology development.
- Digital threats intended to silence or deter women's and gender-diverse people's participation in peace and political processes.
- Chilling effects of online harms, particularly on young women and gender-diverse people.
- Gender digital divides as barriers to equitable inclusion in peacebuilding technologies.

65 Baekgaard, K. (2024). Op. cit.

66 Kakande, A., Achieng, G., Iyer, N., Nyamwire, B., Nabulega, S., & Mwendwa, I. (2021). *Amplified Abuse: Report on Online Violence Against Women in the 2021 Uganda General Election*. Pollicy. https://archive.pollicy.org/wp-content/uploads/2021/08/Amplified-Abuse-Report.pdf

67 Baekgaard, K. (2024). Op. cit.

68 Kayastha, S., & Pokharel, M. (2021). *Identities Experiencing the Internet. Nepal Survey Report*. Body & Data. https://www.apc.org/sites/default/files/identities_experiencing_the_internet_erotics_nepal_report.pdf

69 Fal-Dutra Santos, A., & Pourmalek, P. (2022). Op. cit.

70 The gender digital divide refers to the gap between men, women and gender-diverse people in access to, use of and influence over digital technologies, shaped by social, economic and structural inequalities. See more at: https://www.apc.org/en/glossary/gender-digital-divide

71 Fal-Dutra Santos, A., & Pourmalek. P. (2022). Op. cit.

72 Global Network of Women Peacebuilders & ICT4Peace Foundation. (2021). *Women, Peace and Security and Human Rights in the Digital Age: Opportunities and risks to advance women's meaningful participation and protect their rights. Policy Brief*. https://ict4peace.org/wp-content/uploads/2021/10/WPS-in-the-digital-age_policy-brief_15-October-FOR-LAYOUT-1.pdf

Protection

In addition to implicitly affecting participation, cyberviolence against women and girls, or TFGBV, is also directly and clearly related to the protection pillar of WPS. TFGBV is alarmingly widespread: 81% of women parliamentarians,[73] 73% of women journalists[74] and 38% of women globally[75] report experiencing digital rights violations. UN Women Asia and the Pacific notes that while women and gender-diverse people are already disproportionately affected by TFGBV, these impacts are often exacerbated in conflict and post-conflict settings,[76] an observation that is echoed by activists who argue there is a need to revisit the current framing of TFGBV to better account for these realities.[77] Ethnic and religious minorities, "lower-caste" groups[78] and members of the LGBTQI+ community receive both the most and the worst of digital violence,[79] and 20% of women under 34 report experiencing daily abuse online, underscoring the particular vulnerability of younger women.[80]

While this report focuses on gender-based digital violence within the protection pillar, it is important to acknowledge that protection also encompasses broader women's human rights in digital spaces, including the right to expression, education and access to information. TFGBV can create a "chilling effect", deterring women and gender-diverse people from participating online or in public life – a dynamic closely linked to the gender digital divide – and it constitutes a violation of these broader human rights, underscoring the need for protective measures that go beyond direct violence.

73 Inter-Parliamentary Union. (2016). *Sexism, harassment and violence against women parliamentarians. Issues Brief*. http://archive.ipu.org/pdf/publications/issuesbrief-e.pdf

74 Dhrodia, A. (2021, 13 April). To stop online abuse against women, we must reform digital spaces. *World Wide Web Foundation*. https://webfoundation.org/2021/04/to-stop-online-abuse-against-women-we-must-reform-digital-spaces/

75 Amnesty International. (n/d). *Online Violence*. https://www.amnesty.org/en/what-we-do/technology/online-violence/

76 UN Women Asia and the Pacific. (2023). *Promoting Women's Peace and Security in the Digital World*. https://asiapacific.unwomen.org/en/what-we-do/peace-and-security/promoting-womens-peace-and-security-in-the-digital-world

77 Feminist Internet Research Network. (2024). Reimagining, broadening and expanding TFGBV and transnational solidarity. https://firn.genderit.org/blog/reimagining-broadening-and-expanding-tfgbv-and-transnational-solidarity

78 Kain, D., Narayan, S., Sarkar, T., & Grover, G. (2021). *Online caste-hate speech: Pervasive discrimination and humiliation on social media*. Centre for Internet and Society. https://www.apc.org/sites/default/files/online_caste-hate_speech.pdf

79 Office of the High Commissioner for Human Rights. (2021, 23 March). Report: Online hate increasing against minorities, says expert. https://www.ohchr.org/en/stories/2021/03/report-online-hate-increasing-against-minorities-says-expert

80 PLAN International. (2024, 23 July). Hundreds of girls say they face online harm at least once a month. https://plan-international.org/news/2024/07/23/hundreds-of-girls-say-they-regularly-face-online-harm/

Key issues that are highlighted within the protection pillar include:

- Pervasiveness of cyberviolence and TFGBV against women and gender-diverse people, including those in public life.
- Unique digital threats faced by women in conflict-affected and post-conflict contexts.
- Disproportionate and differentiated threats experienced by marginalised groups in cyberspace.

Prevention

Within the prevention pillar, two major themes emerge in the literature. The first, highlighted by Sharland et al., is gender and online radicalisation.[81] Henshaw identifies three key areas relating to technology and radicalisation: 1) the use of technology by extremist groups to directly facilitate physical and sexual violence against women and other marginalised groups; 2) gender-based patterns of online recruitment by extremist organisations; and 3) the emerging challenge of semiotic violence online, examining the various ways that extremist groups engage with online platforms with the intent of silencing or discrediting women.[82] Research also indicates that online radicalisation efforts often target young men, including minors, placing them at risk of exposure to violence, contact with law enforcement and participation in harmful activities.[83] Acknowledging this dynamic is important alongside examining the risks posed to women and other marginalised groups, as it highlights the broader spectrum of vulnerabilities and consequences associated with online extremism.[84] Baekgaard argues that WPS actors must engage more deeply with these realities, as they contribute to violence and instability in the offline world.[85] The second major theme examines how patterns of digital violence may serve as early warning signals for emerging conflict, with spikes in violence against women indicating escalating tensions.[86]

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

82 Henshaw, A. (2021). *Bringing Women, Peace and Security Online: Mainstreaming Gender in Responses to Online Extremism*. Global Network on Extremism & Technology. https://gnet-research.org/wp-content/uploads/2021/03/GNET-Report-Women-Peace-And-Security.pdf

83 Kimmel, M. (2018). *Healing from Hate. How Young Men Get Into – and Out of – Violent Extremism.* University of California Press. https://doi.org/10.1525/9780520966086

84 Sanil, Y. (2025, 9 May). How Online Spaces Are Fueling Misogyny – And What We Can Do About It. *Welsh Women's Aid.* https://welshwomensaid.org.uk/news/how-online-spaces-are-fueling-misogyny-and-what-we-can-do-about-it/

85 Baekgaard, K. (2024). Op. cit.

86 UN Women Asia and the Pacific. (2020). *Women, Peace & (Cyber) Security: In Asia & Pacific. Action Brief*. https://asiapacific.unwomen.org/sites/default/files/2023-02/ap-wps-221130BLS22555-Peace-and-cyber-insecurity-brief-v03-ENG.pdf

With regards to the prevention pillar, key issues are:

- Online misogynistic radicalisation as a direct threat to women, gender-diverse people and broader peace and security.
- Potential to leverage TFGBV-related data to detect and predict emerging conflict dynamics.

Relief and recovery

Compared to other WPS pillars, relief and recovery remains significantly underexplored in relation to cybersecurity. While Sharland et al. and others have identified it as a priority, the gender-differentiated impacts of cyber incidents have yet to be fully examined within the WPS context. However, relevant insights from humanitarian and digital rights research offer useful entry points.

For example, studies by WILPF and APC highlight how women have specific needs and face specific threats during potential cyber conflicts.[87] Studying the impacts of internet shutdowns on women, they find that women face intersecting harms during shutdowns, including threats to safety, economic security, emotional wellbeing and access to education and communication.[88] Other studies explore the gendered effects of ransomware on health services,[89] the weaponisation of data by malicious actors[90] and state-based over-reach.[91] Each of these can be extrapolated to inform contexts that focus on WPS relief and recovery. UN Women emphasises the potential of context-specific, rights-based and gender-responsive technological solutions to enhance relief and recovery in post-conflict and post-crisis settings,[92] though they do not fully engage with associated challenges. Building on these insights, Millar and Ferrari emphasise the importance of gender-responsive emergency and recovery planning, particularly for cyber incidents affecting critical infrastructure. They note that while all people rely on infrastructure, access and dependence vary across genders and communities, making some services more "critical" for specific groups. Incorporating intersectional, gender-responsive threat modelling, developed by diverse teams across state, private and civil society sectors, can help ensure that relief and recovery strategies are equitable, context-sensitive and effective, systematically including women and gender-diverse

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

88 Ibid.

89 Palacios Ramírez, L., & Camelo, P. (2024). *Ciberataque a Sanitas: Impactos Diferenciales sobre Mujeres Cuidadoras.* Fundación Karisma. https://web.karisma.org.co/wp-content/uploads/2024/03/CIBERATAQUE-SANITAS-2.pdf

90 Pavlova, P. (2024). *Gendered Harms of Data Weaponization. Historical Patterns, New Battlefields, and the Implications for Democracy and National Security.* New America. https://www.newamerica.org/future-security/reports/gendered-harms-of-data-weaponization/

91 Shires, J., Hassib, B., & Swali, A. (2024). *Gendered hate speech, data breach and state overreach.* Chatham House. https://www.chathamhouse.org/sites/default/files/2024-05/2024-05-24-gendered-cyber-harms-shires-et-al_0.pdf

92 UN Women Asia and the Pacific. (2023). Op. cit.

people in planning and implementation.[93] Sharland et al. also highlight gender bias in digital technologies,[94] an underexplored but critical issue with implications for relief efforts shaped by data, automation or AI.

While more work remains to be done in this sense, the differentiated impacts that cyber incidents and gender-unaware emergency responses have on women and people of diverse sexualities and genders is a key issue for cybersecurity with regards to relief and recovery.

State of integration and challenges

Although the literature on the intersections of WPS, cybersecurity and TFGBV is relatively recent, it highlights clear and relevant overlaps. Despite a growing evidence base, years of activist advocacy and the UN Secretary General's annual reports on WPS recognising the role of technology and cyberspace over the past five years,[95] formal integration of these issues remains limited. None of the 10 UN Security Council Resolutions on WPS engage with TFGBV or cybersecurity in any substantive detail.[96] As of 2022, only four WPS NAPs referenced cybersecurity[97] and while 28 included references to ICTs, most were positive references.[98] Similarly, only 14 national cybersecurity strategies referenced gender or women, and most of these did so solely to acknowledge the gender gap in technology sector employment.[99]

The final substantive report of the 2019-2021 Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies welcomed gender perspectives in its discussions, underscoring the importance of narrowing the gender digital divide, promoting meaningful participation and leadership of women in cyber decision-making and adopting capacity-building principles that are gender-sensitive, inclusive and non-discriminatory.[100] In its final report, the 2021-2025 Open-Ended Working Group on security of and in the use of information and communications technologies (2021-2025 OEWG) highlighted calls from states for a gender perspective in addressing ICT threats and the specific risks faced by persons in vulnerable situations, the need for gender-responsive capacity-building

93 Millar, K., & Ferrari, V. (2025). Op. cit.

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

95 UN Women Asia and the Pacific. (2024). Op. cit.

96 Fal-Dutra Santos, A., & Pourmalek, P. (2022). Op. cit.

97 Hofstetter, J.-S., & Pourmalek, P. (2023). *Gendering Cybersecurity through Women, Peace and Security: Gender and Human Rights in National-Level Approaches to Cybersecurity*. Global Network of Women Peacebuilders & ICT4Peace Foundation. https://ict4peace.org/wp-content/uploads/2023/03/Gendering-Cybersecurity-through-WPS-Final-Report_March-2023.pdf

98 Fal-Dutra Santos, A., & Pourmalek, P. (2022). Op. cit.

99 Hofstetter, J.-S., & Pourmalek, P. (2023). Op. cit.

100 General Assembly. (2021). *Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report.* United Nations. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

efforts including through the integration of a gender perspective into national ICT and capacity-building policies, as well as the development of checklists or questionnaires to identify needs and gaps.[101] However, final substantive OEWG reports do not reference WPS in any capacity.

While the WPS agenda has evolved significantly over the years,[102] the literature identifies several key challenges in integrating cybersecurity and technology. The first major challenge is the rapid pace of technological development, which outstrips the speed at which policy can be crafted,[103] making it difficult to stay on top of pertinent issues. Henshaw further highlights that digital issues are often narrowly framed. For example, the gender digital divide is frequently treated solely as a development concern, leading to siloed efforts and limited engagement from WPS actors, who tend to focus on specific types of harm, like conflict-related sexual violence (CRSV).[104] She also notes that some states resist establishing global governance frameworks for cyberspace as they seek to assert national sovereignty in the domain.[105] Moreover, there is tension in the role of the state as a regulator, with many governments using technology to surveil and harass feminist and LGBTQI+ activists.[106] While this is a significant concern, WPS also encounters challenges when some NAPs are developed under regimes that may not prioritise substantive implementation. Despite these obstacles, such challenges should not deter efforts to meaningfully integrate cybersecurity into the WPS agenda.

Limitations and gaps

While the literature has grown substantially over the past two years, major gaps remain in understanding the full scope of issues at the intersection of WPS and cybersecurity. Relief and recovery remain underexplored areas, and women peacebuilders as a distinct group are understudied in the context of digital threats. Additionally, there is a pressing need for more intersectional research that recognises how experiences with and uses of digital spaces are shaped by race, class, caste, sexuality, gender identity, religion, age and other factors. Moreover, much of the literature continues to frame women solely as victims or end-users, overlooking the

101 General Assembly. (2025). *Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025. Draft Final Report*. United Nations. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_10_July_2025.pdf

102 Holvikivi, A., & Smith, S. (2020, 28 September). WPS as evolving and contested terrain: A review of New Directions. *LSE Women, Peace and Security Blog*. https://blogs.lse.ac.uk/wps/2020/09/28/wps-as-evolving-and-contested-terrain-a-review-of-new-directions/

103 Baekgaard, K. (2024). Op. cit.

104 Henshaw, A. (2021). Op. cit.

105 Ibid.

106 Ibid.

roles cisgender men play as architects and perpetrators of digital harm,[107] and the fact that men are disproportionately affected by some forms of TFGBV, such as internet-facilitated sexualised blackmail.[108] Both are omissions that weaken prevention and accountability efforts. Another important gap is the role of gendered disinformation, which, though increasingly studied in other contexts,[109] remains largely unexamined through a WPS lens.[110] Its framing as a security issue is contested, so research should focus cautiously on the specific harms to women and gender-diverse people.

Furthermore, the militarisation of AI and the deployment of autonomous weapon systems (AWS) present emerging challenges to the WPS agenda. The integration of AI in military operations, including drone swarms and lethal autonomous weapons, raises concerns about accountability, bias and the potential exacerbation of gendered violence in conflict zones. For instance, the use of AI-powered drone swarms in Ukraine[111] and the development of autonomous weapons systems by various nations highlight the need for gender-sensitive approaches in military AI governance.[112] These developments underscore the urgency of addressing the gendered implications of military AI within the broader WPS framework.

Together, this growing body of research underscores both the urgency and complexity of integrating cybersecurity and TFGBV concerns into the WPS agenda. While key issues have been identified across all four pillars, sustained investment in research, policy innovation and inclusive governance is essential to ensure gendered cyber threats are meaningfully addressed within peace and security frameworks. These trends and gaps form the analytical foundation for the following section, which examines how NAPs engage with cybersecurity and TFGBV.

107 Hernández Oropa, M. (2023). *Digital Violence: A study of the profiles of perpetrators and survivors of digital sexual violence*. MenEngage Alliance. https://menengage.org/resources/digital-violence-a-study-of-the-profiles-of-perpetrators-and-survivors-of-digital-sexual-violence

108 Coles, S. (2024, 28 June). Understanding and Combating Sextortion: Why Boys Are Disproportionately Affected. *Farrer & Co.* https://www.farrer.co.uk/news-and-insights/understanding-and-combating-sextortion-why-boys-are-disproportionately-affected/

109 Martins, P. (2024). *Placing "gender" in disinformation.* Association for Progressive Communications. https://www.apc.org/sites/default/files/genderDisinformation.pdf

110 https://she-persisted.org/our-work/research-and-thought-leadership/

111 MacDonald, A. (2025, 2 September). AI-Powered Drone Swarms Have Now Entered the Battlefield. *Wall Street Journal*. https://www.wsj.com/world/ai-powered-drone-swarms-have-now-entered-the-battlefield-2cab0f05

112 Mohan, S., & Cho, D. (2024). *Gender and Lethal Autonomous Weapons Systems.* UNIDIR. https://unidir.org/publication/gender-and-lethal-autonomous-weapons-systems/

Analysis of NAPs and RAPs

This section presents findings from an analysis of 34 national action plans and three regional action plans identified through a targeted keyword search using terms such as "cyber", "online", "digital" and "technology". Each document was then reviewed in full and coded across multiple variables to assess how they engaged with cyber-related issues.

The NAPs and RAPs were categorised according to their level of engagement with cybersecurity and/or TFGBV. This was determined by both the frequency of keyword references and the quality of each reference. Quality was assessed based on the depth of discussion, inclusion of concrete policy actions and alignment with WPS pillars. Within each category, key patterns and trends were identified and a substantive content analysis was conducted to determine which issues were being addressed.

The NAPs included in this analysis were: Albania, Argentina, Armenia, the Bangsamoro Autonomous Region of Muslim Minandano (BARMM),[113] Canada, Chad, Colombia, Croatia, Denmark, Estonia, Finland, Gabon, Iceland, Indonesia, Ireland, Italy, Japan, Kenya, Korea, Namibia, Netherlands, Norway, Philippines, South Africa, Sri Lanka, Sweden, Timor-Leste, UAE, the United Kingdom, Ukraine, Uruguay, the United States, Viet Nam and Zimbabwe.

The RAPs included in this analysis were from the Association for Southeast Asian Nations (ASEAN), the North Atlantic Treaty Organization (NATO) and the Southern African Development Community (SADC).

Observations on terminology

Before proceeding to a more structured analysis of the NAPs and RAPs, several broad observations on terminology warrant mention. One notable feature is the variation in how key terms are used across the plan**s**. While some NAPs employ the term "cybersecurity", many do so without a precise definition, and others use broader terms such as "technology", "digital", "online" or simply "cyber" to address similar or overlapping issues. For instance, the Croatian NAP does not use the term "cybersecurity" at all, but references "security risks from natural and technological disasters."[114] Ukraine's plan discusses "digital and information threats",[115] while Uruguay highlights the need for gender-sensitive approaches to "the protection of the civilian population in conflict scenarios and cybersecurity."[116] Although these examples appear to address

113 For the purposes of this report, the BARMM Regional Action Plan on WPS is considered a national action plan, as it does not aim to coordinate action across multiple countries, rather across one region of a country.

114 Croatia National Action Plan. (2019). https://www.wpsnaps.org/app/uploads/2022/12/Croatia-NAP-2-2019-2023.pdf

115 Ukraine National Action Plan. (2020). https://1325naps.peacewomen.org/wp-content/uploads/2024/04/Updated-NAP-1325-until-2025-Edited-English-version.pdf

116 Uruguay National Action Plan. (2019). https://www.wpsnaps.org/app/uploads/2019/09/Uruguay-NAP-2021-2024_spanish_ENG-translation-Google-Translate.pdf

similar concerns, they do so using varied language and conceptual framings. Some of this variance may simply reflect translation differences, but it is important to be aware of this when working to coordinate efforts across and within borders.

Relatedly, the concept of TFGBV is only explicitly named in five plans, those of NATO, Canada, Denmark, the United States and the United Kingdom, all members of the Global Partnership for Action on Online Gender-Based Abuse (Global Partnership).[117] Noting the usage of the term TFGBV is relevant because the concept captures a broader range of digital harms than terms like online violence against women and girls (OVAWG) and explicitly recognises the gendered dimensions of online violence, including impacts on gender-diverse people, though translation and political sensitivities around the word "gender" may affect its uptake.

Furthermore, even plans with a high level of engagement on cybersecurity rarely reference major digital rights frameworks or resolutions, with the exception of members of the Global Partnership. Given the existence of several robust international frameworks on digital rights and the inherently transnational nature of cybersecurity and TFGBV, there are significant opportunities for future NAPs to harmonise their language and explicitly draw on these tools to support cooperation and shared understanding.

Despite the variation in terminology, all plans were assessed using a consistent coding framework, enabling a comparative analysis of their substantive engagement with cyber-related issues. The following section categorises the NAPs and RAPs based on the quality of that engagement.

Levels of engagement

Each of the 37 NAPs and RAPs was categorised into one of three levels based on the extent of their engagement with cyber-related issues: limited engagement (15 NAPs and one RAP); some engagement (11 NAPs and one RAP); and significant engagement (seven NAPs and one RAP). These classifications were determined by both the frequency of references to key terms and the quality of those references.

Limited engagement

The NAPs and RAPs in this category are from Chad, Estonia, Gabon, Iceland, Indonesia, Italy, Japan, Kenya, NATO, Norway, South Africa, Sri Lanka, Sweden, UAE, Viet Nam and Zimbabwe.

Plans categorised as having limited engagement with cybersecurity generally contained two or fewer references to key terms and lacked substantive discussion of the issues.

117 The Global Partnership is an intergovernmental initiative specifically dedicated to addressing TFGBV. It consists of 16 partner countries and works with a multi-stakeholder advisory group composed of TFGBV advocates, leaders and experts from civil society, research and academia, the private sector and international organisations. The coordination of the advisory group is managed by the United Nations Population Fund (UNFPA) and APC.

With few exceptions, most NAPs at this level merely "recognised" cybersecurity as an issue without elaboration or specific policy actions. Recognition typically took one of two forms. First, some briefly mention cybersecurity as a "new" or emerging threat relevant to the agenda, without further detail. Both Estonia[118] and Zimbabwe[119] group cybersecurity alongside climate change and COVID-19 as emergent threats related to UNSCR 1325, while Kenya references the changing nature of crime, including cybercrime.[120] Second, some plans mention cyber, digital or online elements only in relation to other issues. Iceland notes that technology is being used to fuel gender-based violence,[121] South Africa calls on the need for cyber-safety measures in efforts to prevent human trafficking[122] and Norway notes that technology is an important tool in counterterrorism work.[123] This limited engagement reflects a recurring critique of WPS actors adopting an "add women and stir" approach, meaning they advocate only for women's inclusion without addressing the fundamentally gendered nature of security and peace practices.[124] This mistake now seems to be replicated in an "add cyber and stir" approach, in which several NAPs lack a critical engagement with the specific ways cybersecurity intersect with WPS and gender broadly.

The Italian NAP stands out within this category. While it only briefly references online crimes, it uniquely names specific authorities – the police and security forces and judicial institutions – that are responsible for addressing the issue of online harassment,[125] going a step further than many other NAPs with limited engagement. However, its narrow focus on digital violence against women refugees and asylum seekers excludes citizens,[126] revealing a broader tension in WPS: although UNSCR 1325 was originally designed for conflict-affected contexts, gender-based violence is pervasive in all societies.[127] This reflects a substantial challenge for the integration of WPS and cybersecurity, given that most states do not craft WPS policies with a domestic focus, leading to a strong neglect of non-CRSV gender-based violence in many externally oriented NAPs. Given cybersecurity's transnational and ubiquitous

118 Estonia National Action Plan. (2020). https://www.wpsnaps.org/app/uploads/2022/12/Estonia-NAP-3-2020-2025.pdf

119 Zimbabwe National Action Plan. (2023). https://wpsfocalpointsnetwork.org/wp-content/uploads/2024/05/Zimbabwe-UNSCR1325-NAP_Final-170124.pdf

120 Kenya National Action Plan. (2020). https://www.wpsnaps.org/app/uploads/2021/01/Kenya-NAP-2-2020-2024.pdf

121 Iceland National Action Plan. (2025). https://www.government.is/library/01-Ministries/Ministry-for-Foreign-Affairs/PDF-skjol/Iceland%20NAP%20WPS%202025%20-%20final.pdf

122 South Africa National Action Plan. (2020). https://www.wpsnaps.org/app/uploads/2019/09/South-Africa-NAP-1-2020-2025.pdf

123 Norway National Action Plan. (2023). https://www.wpsnaps.org/app/uploads/2024/07/Norway-NAP-5-2023-2030.pdf

124 Dharmapuri, S. (2011). Just Add Women and Stir? *The US Army War College Quarterly Parameters, 41* (1), 456-470. https://www.researchgate.net/publication/265815779_Just_Add_Women_and_Stir

125 Italy National Action Plan. (2020). https://www.wpsnaps.org/app/uploads/2022/12/Italy-NAP-4-2020-2024.pdf

126 Ibid.

127 Whetstone, C., & Luna, K. C. (2024). Op. cit.; Holvikivi, A., & Reeves, A. (2020). Women, Peace and Security after Europe's 'refugee crisis'. *European Journal of International Security, 5*(2), 135-154. https://doi.org/10.1017/eis.2020.1

nature, many NAPs will need to expand their scope to address digital violence domestically and inclusively.

Almost exclusively, NAPs with limited engagement focus solely on the protection pillar, often addressing only the digital aspects of gender-based violence. Notably, both South Africa[128] and Gabon[129] specifically address cybersecurity in relation to human trafficking – a theme that emerges across all engagement levels. Technology-facilitated human trafficking has been studied extensively,[130] with bodies such as the Organization for Security and Co-operation in Europe (OSCE) calling for action to address the problem.[131] The relative absence of this dimension in WPS and cybersecurity literature, despite its presence in many NAPs, offers a valuable opportunity for gender-specific research and alignment across countries and international frameworks focused on trafficking. At the same time, feminist researchers approach the topic of trafficking with caution, recognising that while it is a serious issue, it has also been used to expand state carceral powers and potentially criminalise victims in ways that may conflict with broader feminist justice commitments.

Some engagement

The NAPs and RAPs in this category are from Armenia, Colombia, Croatia, Denmark, Ireland, Korea, Namibia, Netherlands, the Philippines, SADC, Timor-Leste, Uruguay and Ukraine.

NAPs in this category contain two to five unique references to key terms and demonstrate a more substantial level of integration than mere passing mentions. Broadly, most plans recognise one or more key cybersecurity issues and propose specific actions, policies or indicators to address them. Ireland's NAP for example, mimics the language in many of the previous categories, recognising the new challenges to UNSCR 1325, including "cyber-related threats, the availability of new technologies of war and the need to prevent violent extremism," and specifically calls for closing the cybersecurity employment gap as part of this effort.[132] Armenia similarly focuses on women's participation in cybersecurity programs, advocating for cyber-literacy initiatives to enhance protections for women.[133]

There is notable variation in the cyber-related issues prioritised and the mechanisms

128 South Africa National Action Plan. (2020). Op. cit.

129 Gabon National Action Plan. (2020). https://www.wpsnaps.org/app/uploads/2022/12/Gabon_NAP1_french_ENG-translation-Google-Translate.pdf

130 Sarkar, S. (2015). Use of technology in human trafficking networks and sexual exploitation: A cross-sectional multi-country study. *Transnational Social Review, 5*(1), 55-68. https://doi.org/10.1080/21931674.2014.991184; Barney, D. (2018). Trafficking Technology: A Look at Different Approaches to Ending Technology-Facilitated Human Trafficking. *Pepperdine Law Review, 45*(4), 747-748. https://digitalcommons.pepperdine.edu/plr/vol45/iss4/3

131 Organization for Security and Co-operation in Europe. (2024). *Policy action to address technology-facilitated trafficking in human beings*. https://www.osce.org/cthb/579190

132 Ireland National Action Plan. (2019). https://www.ireland.ie/939/Third-National-Action-Plan_1.pdf

133 Armenia National Action Plan. (2022). https://www.wpsnaps.org/app/uploads/2024/07/Armenia-NAP-2-2022-2024.pdf

proposed. Several plans emphasise protection: Denmark,[134] Namibia,[135] SADC[136] and Uruguay[137] offer in-depth references to digital gender-based violence, though only Denmark explicitly uses the term TFGBV. The Netherlands also focuses on digital harassment, specifically noting that women human rights defenders and peacebuilders face disproportionate risks.[138] The Philippines NAP dedicates an entire action point to cybersecurity, focusing heavily on women's inclusion in cybersecurity planning, design, governance and law enforcement.[139] Ukraine stands out for directly addressing information threats, committing to develop and implement plans that meet the diverse needs of women and girls across different ages.[140]

Some plans in this category adopt a broader approach, referencing cybersecurity generally, rather than specific issues or concerns. The Republic of Korea draws attention to the importance of WPS in cyberspace, and pledges to coordinate and support international cooperation to integrate cyber concerns in WPS.[141] The SADC Plan contributes a unique a structural perspective, noting that peace and security are not confined to conflict or post-conflict contexts and are shaped by everyday structural insecurities, such as poverty, cybercrime and gender-based violence, highlighting the need for all NAPs to include not only external actions, but internal reflections and priorities as well.[142]

Overall, NAPs in this category reflect broader and more substantive engagement with cybersecurity, particularly through the lenses of participation and protection. Notably, Uruguay, Ukraine and Croatia are the only plans in the dataset to address relief and recovery in any capacity. While these plans do not represent comprehensive integration of cybersecurity and WPS, they provide useful insights into how countries might engage with specific issues relevant to their contexts.

134 Denmark National Action Plan. (2025). https://um.dk/en/-/media/websites/umen/danida/results/evaluation-of-development-assistance/2025wpsstudy.ashx

135 Namibia National Action Plan. (2019). https://wpsfocalpointsnetwork.org/wp-content/uploads/2021/07/Namibia-2019-2024.pdf

136 SADC Regional Action Plan. (2018). https://wpsfocalpointsnetwork.org/wp-content/uploads/2021/07/RAP-2018-2022-SADC.pdf

137 Uruguay National Action Plan. (2019). Op. cit.

138 Netherlands National Action Plan. (2021.) https://wpsfocalpointsnetwork.org/wp-content/uploads/2021/07/Netherlands-2021-2025.pdf

139 Philippines National Action Plan. (2023). https://1325naps.peacewomen.org/wp-content/uploads/2025/02/NAPWPS-2023-2033-DIGITAL.pdf

140 Ukraine National Action Plan. (2020). Op. cit.

141 Republic of Korea National Action Plan. (2024). https://wpsfocalpointsnetwork.org/wp-content/uploads/2024/09/4th-NAP-Republic-of-Korea.pdf

142 SADC Regional Action Plan. (2018). Op. cit.

Case study: Colombia

Publication year: 2024

Period: 2024-2034

Iteration: First

Colombia's National Action Plan (NAP) stands out as a unique and exemplary case in the Women, Peace and Security (WPS) landscape, for both its content and the inclusive process through which it was developed. It was built on over two decades of sustained advocacy by Colombian women's organisations,[143] and was shaped through a six-month national consultation involving over 1,500 women from diverse backgrounds, including Indigenous, Afro-Colombian and LBTQIA+ communities, and various age groups.[144] Inclusivity was central to this process, making Colombia's approach distinct among national implementations of UNSCR 1325.

This is particularly evident in the NAP's cyber-related provisions, which directly reflect the lived experiences and priorities of Colombian women. The plan commits to a risk prevention program that integrates care strategies, digital security and practical tools to combat sexual and gender-based violence against women and girls, specifically highlighting peace signatories and Afro-Colombian, Indigenous and LBT women.[145] The NAP further addresses the gender digital divide by promoting digital skills training for women in both urban and rural conflict-affected areas, supporting their entry into the labour market.[146] It also includes targeted cybersecurity training for women in the military as a strategy to prevent gender-based violence in contexts shaped by ongoing urban and rural conflict.[147]

The importance of grounding both broader NAP development, as well as cyber-specific provisions, in the direct experiences of women and people of diverse sexualities and genders in a given context cannot be overstated. Women from different contexts interact with technology in different ways,[148] and as such, have different cybersecurity needs. Colombia's NAP may not be the most expansive in its engagement with cybersecurity and technology, but it may well be the one that most accurately captures the specific needs of the women impacted, given the extensive consultations that were carried out during its development. With that said, it is worth noting that many CSOs in Colombia have expressed frustration at the lack of follow-up on the plan, emphasising that a NAP is only effective if it is implemented.[149]

143 ABColombia. (2023, 25 May). Advances in the Colombian National Action Plan of UN Resolution 1325: Women, Peace, and Security. *ABColombia.* https://www.abcolombia.org.uk/advances-in-the-national-action-plan-resolution-1325/

144 NIMD. (2024, 10 December). Breaking New Ground: Colombia's Inclusive Journey to a National Action Plan. *NIMD.* https://nimd.org/breaking-new-ground-colombias-inclusive-journey-to-a-national-action-plan/

145 Colombia National Action Plan. (2024). https://wpsfocalpointsnetwork.org/wp-content/uploads/2025/01/articles-397916_recurso_2.pdf

146 Ibid.

147 Ibid.

148 Iyer, N., Nyamwire, B., & Nabulega, S. (2020). *Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet.* Pollicy. https://www.apc.org/sites/default/files/Report_FINAL.pdf

149 ABColombia. (2024, 8 March). International Women's Day 2024: Update on the Implementation of UNSCR 1325 and the NAP. *ABColombia.* https://www.abcolombia.org.uk/international-womens-day-2024-update-on-the-implementation-of-unscr-1325-and-the-nap/

Significant engagement

The NAPs and RAPs in this category are from Albania, Argentina, ASEAN, the BARMM, Canada, Finland, the United Kingdom and the United States.

The significant engagement category includes NAPs that feature five or more unique references to key cyber-related terms and take a more holistic approach to cybersecurity. These plans offer both extensive recognition of cybersecurity as a WPS issue and multiple concrete actions addressing a variety of digital threats and opportunities. With the exception of Finland, all plans in this category engage with cybersecurity across the three WPS pillars of participation, protection and prevention, reflecting a more comprehensive approach to integrating cyber concerns into WPS agendas. With that said, it is important to note that detailed commitments in NAPs do not always translate into implementation, particularly when governments change.

Participation

NAPs in this category are distinct in their emphasis on women's meaningful inclusion in digital policy, leadership in cybersecurity and closing the gender digital divide. Several explicitly link these efforts to broader national security and digital inclusion goals. Argentina stands out for its detailed focus on gender gaps in cybersecurity leadership. It calls for gender-disaggregated data collection on public administration roles, including in the cybersecurity, cyber diplomacy and defence sectors,[150] and commits to championing these values in international forums. Finland defends the right of all women and girls to a safe online environment, referencing concrete examples of doing so as the co-leader of the technology and innovations action group with UN Women.[151] The ASEAN plan commits to women's participation in responses to cybersecurity[152] and launching programmes to close the gender digital divide.[153] The United States plan explicitly includes US cyber command, addressing the gender dimensions of the cyber domain and the recruitment and retention of women and girls in STEM fields, and provides explicit examples of doing so.[154] Despite differing approaches, these NAPs share two notable characteristics: 1) their recommendations are concrete and elaborated in significant detail; and 2) they frame gendered cybersecurity concerns as relevant not only within WPS but across broader security and governance agendas.

150 Argentina National Action Plan. (2021). https://wpsfocalpointsnetwork.org/wp-content/uploads/2023/04/Argentina.pdf

151 Finland National Action Plan. (2023). https://1325naps.peacewomen.org/wp-content/uploads/2024/04/UM_2023_13.pdf

152 ASEAN Regional Plan of Action. (2022). https://asean.org/wp-content/uploads/2022/11/32-ASEAN-Regional-Plan-of-Action-on-Women-Peace-and-Security.pdf

153 Ibid.

154 United States National Action Plan. (2024). https://1325naps.peacewomen.org/wp-content/uploads/2024/04/U.S.-Strategy-and-National-Action-Plan-on-Women-Peace-and-Security.pdf

Protection

Protection from digital and cyber-related violence is a central concern across all seven plans in this category. These NAPs provide more expansive definitions of digital violence than those in lower-engagement categories and often situate them within the context of broader security threats. Canada and the United States are particularly explicit. Canada warns of escalating online attacks against women human rights defenders, including Indigenous land defenders and 2SLGBTQI+ (two-spirit,[155] lesbian, gay, bisexual, transgender, queer, intersex and other sexual orientations, gender identities and expressions) communities, linking TFGBV to wider anti-feminist and authoritarian movements.[156] The US is unique in framing online misogyny and gendered disinformation as national security threats, emphasising their impact on women public figures and the normalisation of hate-fuelled violence online.[157] Finland includes an explicit section dedicated to online gender-based violence[158] and highlights the need for specific considerations to be made in fragile operating environments and conflicts.[159] Like the UK,[160] Albania also connects cyber protection to broader conflict and insecurity contexts, but proposes measures to prevent and report violence.[161] The BARMM plan also stands out for framing GBV as a continuum that occurs both online and offline. This dual recognition situates digital harms within the broader landscape of insecurity, reinforcing the indivisibility of online and offline threats.[162]

Collectively, these NAPs reflect a shared understanding that protection from digital harms is essential to security in the digital age and must be integrated into broader protection frameworks.

Prevention

Prevention is more prominently addressed in this category than in plans with lower levels of engagement, particularly in relation to early warning systems, disinformation and emerging security challenges. While Albania's NAP is less detailed, it still calls for integrating gender perspectives into digital conflict-prevention policies.[163]

155 Two-spirit is a term used to describe an Indigenous person who embodies both masculine and feminine qualities, often encompassing a spiritual and gender identity outside the binary.

156 Canada National Action Plan. (2024.) https://www.international.gc.ca/transparency-transparence/assets/pdfs/women-peace-security-femmes-paix-securite/2023-2029-foundation-peace-fondation-paix-en.pdf

157 United States National Action Plan. (2024). Op. cit.

158 Finland National Action Plan. (2023). Op. cit.

159 Ibid.

160 United Kingdom National Action Plan. (2023). https://assets.publishing.service.gov.uk/media/645d2d94ad8a03001138b33c/uk-women-peace-security-national-action-plan-2023-2027.pdf

161 Albania National Action Plan. (2023). https://1325naps.peacewomen.org/wp-content/uploads/2025/02/Albania-second-NAP-2024-5.pdf

162 BARMM Regional Action Plan. (2023). https://bwc.bangsamoro.gov.ph/wp-content/uploads/2024/09/UNW-1215-BARMM-Action-Plan-FULL-REPORT.pdf

163 Albania National Action Plan. (2023). Op. cit.

ASEAN promotes the use of early warning mechanisms for cybersecurity threats and emphasises the importance of gender-sensitive analysis, with specific attention to marginalised groups.[164] The BARMM plan distinguishes itself by including specific indicators for measuring gender-responsive cybersecurity policies and introducing a unique action item to support research on the intersection of WPS and cybersecurity.[165] These commitments extend beyond the scope of most NAPs, signalling a strong institutional interest in building evidence and accountability mechanisms around digital threats. The UK and the US both highlight the intersection of digital threats with violent extremism and geopolitical instability. The UK broadens its threat lens beyond countering violent extremism to include the manipulation of digital platforms by belligerent actors,[166] while the US uniquely emphasises the threat of online hate to democratic institutions and public trust.[167] Canada is also singular among all NAPs in the sample, specifically articulating a policy alignment with their National Cyber Security Strategy, demonstrating a strong commitment to integrating gender and cybersecurity into their "ecosystem of policies".[168]

Together, these plans reflect a growing recognition that effective prevention in the digital age demands anticipatory action, gender-responsive policy integration and an understanding of how cyber threats can undermine both peace and democratic resilience.

164 ASEAN Regional Action Plan. (2022). Op. cit.

165 BARMM Regional Action Plan. (2023). Op cit.

166 United Kingdom National Action Plan. (2023). Op. cit.

167 United States National Action Plan. (2024). Op. cit.

168 Canada National Action Plan. (2024). Op. cit.

Case study: ASEAN

Publication year: 2022

ASEAN offers a strong example of the important role regional action plans can play in coordinating WPS efforts across multiple countries, particularly in response to transnational issues like cybersecurity. Several countries analysed in this dataset, including the Philippines, Indonesia and Viet Nam, are ASEAN member states and have likely been shaped by the region's collective priorities and commitments to cybersecurity.

The ASEAN Regional Plan of Action on WPS reflects a multifaceted and forward-looking approach to integrating gender into emerging security challenges. Notably, it includes commitments to enhance early warning systems, address cybercrime and online gender-based violence and strengthen the participation of women in responses to both traditional and non-traditional threats, such as violent extremism and digital insecurity.

A key driver of ASEAN's progress in this area has likely been its close partnership with UN Women.169 This initiative has facilitated regional platforms, technical assistance and stronger links between civil society and policy-making spaces. UN Women Asia & the Pacific has also emerged as a leader in WPS and cybersecurity, with a detailed strategy encompassing short, medium and long-term goals and consistent efforts to understand and address the gendered dimensions of cyber threats.[170] In a region where digital harms cross borders and affect peacebuilding at all levels, ASEAN's approach highlights the value of regional coordination, sustained partnerships and inclusive, gender-responsive policy design.

169 UN Women Asia and the Pacific. (2024). *Women, Peace and Security in ASEAN: Project Explainer.* https://asiapacific.unwomen.org/sites/default/files/2024-03/wps-asean_project_explainer_20240306.pdf

170 UN Women Asia and the Pacific. (2024). *Joint Roadmap for Women's Economic Empowerment and Digital Inclusion in Asia and the Pacific.* https://asiapacific.unwomen.org/sites/default/files/2024-01/ap-c571-Joint-Roadmap.pdf

Conclusion

This analysis reveals a growing awareness among states and regional actors of the relevance of cybersecurity for women's security and inclusion. However, it also underscores persistent gaps in the depth, coherence and scope of that engagement. While a small number of action plans – such as those from Argentina, Canada, the United Kingdom and ASEAN – demonstrate more robust engagement across multiple pillars and include concrete, gender-responsive policy actions, the majority address cyber issues only superficially, if at all. In contrast to the literature, which highlights the severity and complexity of cyberviolence and explores cybersecurity's multifaceted relevance to peace and security, most action plans continue to underexplore these issues. Although many plans recognise the importance of addressing digital dimensions of gender-based violence, more complex challenges – such as online misogynistic radicalisation or the potential of TFGBV-related data for early warning and conflict prevention – receive little to no attention.

Encouragingly, several plans have begun to address women's underrepresentation in cybersecurity policy making and the digital workforce, aligning with calls for structural inclusion. Yet, threats to women's participation in peacebuilding and political life and the distinct vulnerabilities they face in conflict-affected settings remain inconsistently addressed. Overall, while a handful of NAPs offer promising models for more holistic and gender-responsive engagement with cyber issues, the field remains in its early stages. To meaningfully advance in the digital age, future plans must move beyond token references and explicitly engage with the gendered dimensions of digital harm, power and exclusion.

Getting TFGBV into the US National Action Plan

Publication year: 2022

Two former US government officials, both involved in drafting the current US National Action Plan on WPS, shared reflections on how TFGBV came to be so prominently addressed in the document, as well as thoughts on subsequent implementation.

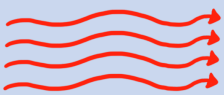
Leadership and leverage
High-level political will was essential. Backing from the administration itself created the space to meaningfully include TFGBV, while civil society "champions" who had entered government helped push the issue forward.

Partnerships and collaboration
The Global Partnership for Action on Gender-Based Online Harassment and Abuse played a foundational role, generating momentum for deepening US integration of TFGBV in bilateral and multilateral foreign policy and security priorities and creating opportunities for other countries to follow suit.

Balance and integration
TFGBV was not treated as a standalone issue but woven throughout the NAP's broader priorities. Integrating digital threats without overshadowing other WPS commitments was a key goal.

Building buy-in
Engaging sceptical stakeholders through briefings, testimonies from survivors and lived-experience experts and creative outreach was critical. Making the case that TFGBV is relevant to national security and WPS goals helped garner broader support.

From policy to practice
Translating TFGBV into WPS language and grounding it in strong evidence from academia and civil society was vital. Equally important was ensuring that commitments are implementable, measurable and not merely aspirational.



Conclusion and recommendations

This analysis underscores both the growing recognition of cybersecurity and technology-facilitated gender-based violence within the Women, Peace and Security agenda and the significant gaps that remain in policy and practice. While a handful of national and regional action plans offer promising models of more holistic and gender-responsive engagement, most continue to treat digital threats superficially or in isolation from broader peace and security concerns. Meaningful progress requires a concerted, multi-level effort to deepen understanding, harmonise terminology and integrate gendered digital harms into all pillars of WPS. The following recommendations aim to guide key actors in translating these insights into coordinated and impactful action.

Recommendations for WPS actors

The Women, Peace and Security agenda must evolve to meet the realities of the digital age. Digital threats are no longer peripheral; they are core to how women and gender-diverse individuals experience insecurity, exclusion and violence.

Multilateral WPS actors (i.e. UN Women, OSCE, AU, ASEAN, EU, NATO)

- *Convene cross-sector dialogues between WPS experts and digital rights experts to improve mutual literacy.* Bring together WPS, digital rights and cybersecurity actors to harmonise language across NAPs and RAPs, reducing fragmentation and enabling clearer cooperation on transnational cyber harms.
- *Leverage WPS frameworks to inform international legal and accountability mechanisms.* Use WPS mandates and networks to advocate for gender-responsive data protection laws, privacy rights and cross-border legal cooperation addressing TFGBV and digital violence. Encourage treaty bodies and international courts to recognise TFGBV as a rights violation and security issue.[171]
- *Promote gender-responsive cybersecurity integration through regional WPS mechanisms.* Build on models such as the recent efforts by ASEAN and NATO. These organisations can use their convening power to align and encourage member states to adopt provisions in their own NAPs.
- *Bridge the gap between WPS and digital rights frameworks.* Encourage the referencing of key digital rights instruments (e.g., UN HRC Resolution 47/16 and CEDAW GR 39) and cybersecurity strategies in WPS NAPs and policy documents. Facilitate joint trainings for WPS actors on digital rights standards and vice versa.
- *Support perpetrator-focused research and programming on TFGBV and digital violence.* Fund and promote programming that addresses root causes of TFGBV, including online radicalisation, misogynistic cultures and impunity.

171 Association for Progressive Communications et al. (2024). *Global Call to Action to Address Technology-Facilitated Gender-Based Violence.* https://www.apc.org/sites/default/files/call-to-action-to-address-tf-gbv_csw-2024.pdf

Promote educational initiatives that target harmful behaviours, and expand cyber literacy curricula to foster responsibility and empathy online.[172]

National governments developing or implementing NAPs

- *Conduct inclusive, intersectional consultations.* Engage civil society groups representing women, LGBTQI+ people, youth, persons with disabilities and digital rights communities, especially in conflict-affected and marginalised areas. These groups can provide meaningful insights on their specific needs with regards to protections in digital spaces, in addition to expertise and research on cyber-incidents and threats at a national level. Use their insights to ground cyber-related NAP provisions in lived realities and local contexts.
- *Include explicit, measurable and resourced cyber commitments in WPS NAPs.* Define cyber priorities, assign institutional responsibilities, allocate funding and develop indicators to track progress. Integrate cyber components into all WPS pillars, especially under-addressed areas like relief/recovery and prevention.
- *Broaden the definition of security and cybersecurity in NAPs to reflect the realities of digital life.* Recognise that digital threats affect women and gender-diverse people within national borders, not just in foreign policy or conflict zones. Domestic digital harms should be addressed as legitimate WPS concerns.
- *Institutionalise cross-ministry collaboration.* Ensure NAP implementation bodies work with cybersecurity, ICT and justice ministries and actively include mechanisms for meaningful participation of women, LGBTQI+ people, youth, persons with disabilities and digital rights communities. Collaboratively develop consistent language within governments and national protocols for responding to TFGBV, addressing domestic digital harms and promoting equitable access to digital technologies, recognising that participation in governance, education and society depends on closing the gender digital divide.
- *Promote diversity and inclusion across cybersecurity, technology and security sectors.* Governments should prioritise workforce diversity and inclusion across their cybersecurity, technology and security ministries. This includes promoting gender diversity on all teams, particularly in roles related to cybersecurity, content moderation and AI development, as diverse teams are better equipped to identify and mitigate gender biases in technology and prevent potential harms.
- *Fund intersectional research on violence in digital spaces.* This research should examine how experiences and uses of technology are shaped by race, class, caste, sexuality, gender identity, religion, age and other social factors, providing evidence to inform more inclusive and effective WPS policies and cybersecurity strategies.

172 Feminist Internet Research Network. (2023, 24 August). Policy recommendations from FIRN research. *GenderIT.org.* https://genderit.org/articles/policy-recommendations-firn-research

Civil society and peacebuilders

Civil society actors have led critical work in documenting the gendered impacts of digital violence, developing survivor-centred resources and advancing policy solutions. Research by CSOs has provided essential evidence of how cyber incidents, TFGBV and digital harms affect women, gender-diverse individuals and peacebuilders in diverse contexts. To build on this leadership, civil society actors can continue to drive change while calling on national governments and multilateral institutions to support and scale their efforts.

- *Continue documenting and disseminating evidence on digital harms and responses.* Civil society should be recognised for its essential role in producing knowledge about the gendered impacts of digital threats especially in conflict-affected and underrepresented contexts. Ongoing research should be resourced and amplified by multilateral and national actors.
- *Facilitate cross-sector collaboration and bridge building.* Civil society can foster dialogue and joint initiatives between peacebuilders, digital rights advocates and cybersecurity professionals. These partnerships help identify shared threats, exchange technical and contextual knowledge and design responsive and inclusive strategies.
- *Amplify local and marginalised voices in global policy spaces.* Civil society organisations should continue advocating for meaningful participation of women, LGBTQI+ individuals, Indigenous communities and conflict-affected populations in digital policy forums and WPS processes, while calling on states and multilateral bodies to create accessible and inclusive entry points for engagement.
- *Develop and share practical safety resources.* Building on existing tools, civil society can continue to create localised, culturally relevant and multilingual resources for digital self-protection, particularly for women peacebuilders, human rights defenders and at-risk communities operating in fragile contexts.

Recommendations for digital rights actors

Cybersecurity is peace and security work. Digital rights communities must actively engage with WPS frameworks and conflict-affected populations.

International cybersecurity and digital rights bodies

- *Mainstream WPS into digital governance forums.* Advocate for WPS and gender language to be included in the discussions and outcomes of the UN Global Mechanism on Developments in the Field of ICTs,[173] the Internet Governance Forum (IGF), the International Telecommunication Union (ITU) and Human Rights Council cyber-related sessions. Call for dedicated

173 This mechanism is the process states agreed on upon the end of the OEWG's mandate. Payne, R. (2025, 24 July). The OEWG Ends and a New UN Cybersecurity Permanent Mechanism Is Born. *Global Partners Digital*. https://www.gp-digital.org/the-oewg-ends-and-a-new-un-cybersecurity-permanent-mechanism

TFGBV tracks or working groups at these events.

- *Include WPS voices in global cybersecurity policy design.* Invite WPS organisations, especially from the Global South, to consultations on digital regulation, platform governance, AI ethics and cybercrime legislation. Provide funding and capacity support to enable meaningful participation.
- *Integrate WPS into global digital governance agendas.* Leverage WPS language and framing to advocate for the inclusion of gender in global forums such as the UN global mechanism on cybersecurity, the IGF and Human Rights Council processes.
- The Global Partnership specifically, should focus on supporting its current members in integrating TFGBV into their foreign policy and security priorities, while generating momentum for other member countries to take similar action. The Partnership can play a critical role in shaping global norms, fostering diplomatic collaboration, connecting siloed agendas and promoting multi-stakeholder engagement, ensuring that commitments to women's meaningful participation in governance and online spaces are upheld and effectively implemented.
- *Map policy intersections and align strategies.* Analyse existing NAPs and cybersecurity policies to identify alignment opportunities, such as linking WPS implementation plans to national cybersecurity strategies or regional cyber capacity-building initiatives.

National governments (cybersecurity, ICT or digital ministries)

- *Implement gender provisions across the board.* While NAPs are a strong starting point for harmonising cybersecurity and gender approaches, it should not be the only place it is done. Gender considerations should be built into cybersecurity strategies and all other digital policies and practices.
- *Collaborate with WPS focal points and ministries* to identify where cybersecurity, TFGBV and gender policy intersect**.** Build joint initiatives that bring together cybercrime units, gender ministries and civil society to identify gaps and responses.
- *Develop and enforce regulation* that holds platforms and digital service providers accountable for preventing and responding digital threats. The private sector is notably absent from conversations on WPS, but that does not mean they are not relevant actors. These actions may include:
  - » Mandating human rights due diligence with a gender perspective, including specific assessments of gendered risks in digital environments.
  - » Providing explicit guidance to tech companies on how to implement rights-respecting practices and data protection measures for women and gender-diverse people.
  - » Drawing on WPS principles, including participation, protection and prevention, to guide their regulation of digital technologies and understand the different areas where efforts might be needed.

Civil society organisations

- *Support the creation of shared multilingual terminology sets* developed in collaboration with women peacebuilding experts to bridge vocabulary gaps across WPS and cybersecurity fields.
- *Build bridges between local peacebuilders and digital rights advocates.* Host cross-sector dialogues and regional meetings to share expertise, identify common threats and exchange knowledge on how to leverage existing frameworks.

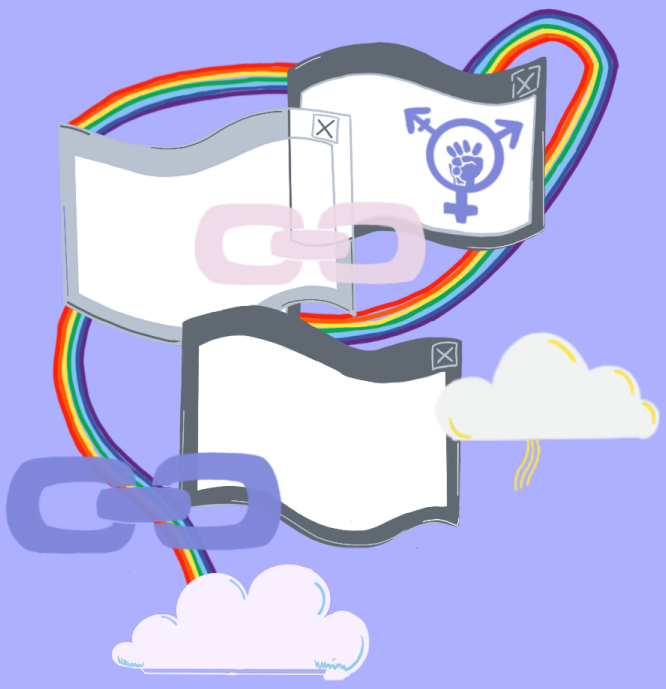
Recommendations for technology companies

Technology companies are not currently included in research or practice regarding WPS and cybersecurity, yet meaningful progress cannot be achieved without their active participation. Social media companies, in particular, have an obligation to ensure digital spaces are safe, inclusive and accessible to all, including through effective consideration of the gender-specific impact of their activities.[174]

- *Invest in workforce diversity and inclusion.* Promote gender diversity on all teams, especially in roles related to cybersecurity, content moderation and AI development. Diverse teams are better equipped to identify and address gender biases in technology and potential harms.
- *Integrate gender-responsive design and safety features.* Proactively design products and services with a gender lens to mitigate risks of online harassment, abuse and exclusion. Incorporate safety tools such as robust content moderation, reporting mechanisms and privacy protections that specifically address the vulnerabilities of women, gender-diverse individuals and marginalised groups.
- *Ensure that redress and reporting mechanisms are accessible and effective.* Social media platforms should ensure that reporting mechanisms are easily findable on their platforms and available in a wide variety of languages and ensure that there is sufficient staffing to address reports of TFGBV as they arise. Content takedown requests in particular should be urgently responded.[175]
- *Collaborate with WPS Actors and civil society.* Establish partnerships with WPS stakeholders, digital rights organisations and peacebuilders to better understand the specific digital threats faced by these communities. Co-create solutions informed by the lived experiences of users, ensuring inclusivity and cultural sensitivity.
- *Support gender-responsive research and innovation.* Fund and participate in interdisciplinary research on TFGBV, digital security and the intersection of technology with peace and security agendas. Innovate technological solutions that enhance digital safety, such as AI-driven abuse detection tools calibrated for gender sensitivity.

174 Cannataci, J. (2019). Op. cit.

175 Feminist Internet Research Network. (2023, 24 August). Op. cit.



APC
ASSOCIATION FOR
PROGRESSIVE
COMMUNICATIONS