

November 2025



ACKNOWLEDGEMENTS

The research team would like to thank the many people who generously contributed their time and insights to this report.

The research team would also like to acknowledge and thank Meg Selianakis for her work on a background desk review during her internship at HAG.

Research team: Sara Phillips, San May Thu, Beth Eggleston

Editor: Aoiffe Corcoran

Copy editor: Campbell Aitken

Graphic design: Jenny Moody, A&J Moody Design

Cover photo: Owl Illustration Company on Unsplash

Disclaimer: This publication was funded by the Australian Government through the Australian Civil-Military Centre. The views expressed in this publication are the authors' and not necessarily those of the Australian Government.

About the project

This is one in a series of three thematic reports. It is part of a two-year project that aims to strengthen engagement on the United Nations' Women, Peace and Security (WPS) Agenda at national, regional and international levels. It also aims to deliver insights and data to the Australian Government on Australian civil society perspectives on WPS abroad and domestically, supporting future implementation ambitions for the Australian Second National Action Plan on Women Peace and Security 2021-2031. It is supported by the Australian Government through the Australian Civil-Military Centre.

CONTENTS

Acknowledgements.....	2
Abbreviations	4
Executive summary	5
1. Introduction	6
2. Research methodology	11
3. Understanding The impacts of gendered disinformation on peace and security	13
4. Emerging opportunities and considerations for NAP implementing agencies	18
Endnotes.....	22
Bibliography	24
Annex: Advancing the WPS Agenda in Cybersecurity and Protection of Civilians Workshops	27
Sydney Workshop Program	27
Melbourne Workshop Program	29

ABBREVIATIONS

AFP	Australian Federal Police
APC	Association for Progressive Communications
DFAT	Department of Foreign Affairs and Trade
EIGE	European Institute for Gender Equality
EIU	Economist Intelligence Unit
GBV	Gender-Based Violence
Global Partnership	Global Partnership for Action on Gender-Based Online Harassment and Abuse
ICFJ	International Center for Journalists
ICTs	Information and Communication Technologies
IPU	Inter-Parliamentary Union
ITU	International Telecommunication Union
LGBTQIA+	Lesbian, Gay, Bisexual, Transgender, Gender Diverse, Intersex and Queer
NAP	Australian Second National Action Plan on Women Peace and Security 2021-2031
NDI	National Democratic Institute for International Affairs
NGO	Non-Governmental Organisation
OEWG	Open-Ended Working Group
OHCHR	Office of the High Commissioner for Human Rights
RCRC	Red Cross Red Crescent
TfGBV	Technology-facilitated Gender-Based Violence
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNSC	United Nations Security Council
WPS	Women, Peace and Security
WRO	Women's Rights Organisation

GLOSSARY

Cybersecurity: the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality.¹

Misinformation: incorrect or false information that is presented as fact. It is not necessarily intended to deceive.

Disinformation: incorrect or false information that is deliberately intended to deceive.

EXECUTIVE SUMMARY

2025 marks 25 years since UN Security Council Resolution 1325 on Women, Peace and Security (WPS). Yet, the intersection of gender and cybersecurity—especially in crisis-affected contexts—remains largely overlooked. None of the 10 UNSC resolutions on WPS mention cybersecurity, and Australia's National Action Plan on WPS and Cyber Security Strategy barely address gendered cyber threats. WPS and cybersecurity integration represents both an important knowledge gap and opportunity. This report doesn't explore all possible avenues of integration between WPS and cybersecurity. Instead, it maps out how the WPS Agenda can be applied to gendered disinformation and identifies key opportunities for integration.

Who is this for?

- **NAP implementing agencies** – Targeted recommendations aligned with Australia's NAP outcome areas.
- **Civil society organisations and networks** – Support advocacy to address gendered cyber threats in peace and security.
- **Technology companies** – Insights for curbing cyber impacts on women's leadership and participation.

Why is this important?

Gendered disinformation, often part of tech-facilitated gender-based violence, can escalate to physical harm, silencing women leaders, journalists, and human rights defenders. In crisis settings, disinformation undermines humanitarian and security efforts, amplified by digital platforms.

Emerging opportunities and considerations for NAP implementing agencies

- 💡 **Safeguard digital participation and public presence of women peacebuilders and leaders**
Support women peacebuilders with access to digital tools, training, and justice mechanisms
- 💡 **Strengthen internal digital resilience and safety through staff training and targeted support**
Train staff in government and civil society organisations to spot and report disinformation; provide tailored digital security support to public-facing staff at risk of gendered disinformation and other online threats
- 💡 **Deepen and elevate advocacy and leadership**
Convene stakeholders across sectors; support implementation of the UN Guiding Principles on Business and Human Rights
- 💡 **Strengthen access to reliable, relevant information in crisis settings by supporting media, women's rights organisations, journalists and local communicators**
Fund trusted local media and communicators; build community-level 'information resilience' ecosystems; improve rapid response verification and counter-messaging capacity; integrate information support into humanitarian responses
- 💡 **Super-charge regional collaboration**
Expand joint initiatives on gender, peace and cybersecurity by building on successful efforts and sharing lessons learnt
- 💡 **Engage diverse civil society expertise**
Commission contextualised research.

1. INTRODUCTION

This year marks the 25th anniversary of United Nations Security Council (UNSC) resolution 1325. In formalising the Women, Peace and Security (WPS) Agenda, UNSC resolution 1325 affirmed the importance of women's participation and the inclusion of gender perspectives in peace negotiations, humanitarian planning, peacekeeping operations, and post-conflict peacebuilding and governance. The UNSC has since adopted nine more resolutions on WPS, including on women's participation and inclusion in peacebuilding, the prevention of and response to conflict-related sexual violence, and the integration of WPS, counterterrorism and countering violent extremism agendas. However, there has been little focus on the representation and participation of women and gender-nonconforming individuals in cybersecurity and the gendered impacts of cyberwarfare and other cyber threats in conflict and crisis-affected settings. WPS and cybersecurity integration represents both an important knowledge gap and opportunity.

Policies and operations that pertain to the WPS Agenda do not sufficiently integrate the risks posed to women and girls from cybersecurity threats. Cybersecurity is an emerging concern in informal UNSC settings such as Arria-formula meetings, and in other UN forums such as the Open-Ended Working Group (OEWG) on Information and Communication Technologies (ICTs). The [UN Guiding Principles on Business and Human Rights](#) also provide a framework for corporate responsibility to protect human rights, which is critical given the private sector's major role in ICTs. However, these principles are limited to ICT forums, and there is no evidence of their integration into wider security agendas. It is significant that none of the 10 UNSC resolutions that make up the WPS Agenda specifically address cybersecurity or the gendered impacts of cyber-attacks and warfare.

Who is this report for?

- **NAP implementing agencies.** The report offers targeted recommendations for NAP implementing agencies, aligned with the four outcome areas of Australia's NAP.
- **Civil society organisations and networks:** The report can be used to raise awareness and strengthen advocacy around the gendered impacts of cyber threats and disinformation in peace and security contexts.
- **Technology companies.** The report can serve as valuable input into discussions with the private sector on curbing cyber impacts on women and undermining women's leadership, credibility and participation in conflict prevention.

Why is this important?

Gendered disinformation, often part of technology-facilitated gender-based violence, can escalate from online threats to physical harm, driving women out of public life and leadership. It disproportionately targets women leaders, journalists, and human rights defenders, silencing voices and deterring participation in peacebuilding and democratic processes. By eroding trust in women leaders, it weakens social cohesion and undermines democracy. In crisis contexts, disinformation further obstructs humanitarian and security efforts, amplified by social media and online platforms.

Australia's second [National Action Plan on Women, Peace and Security 2021–2031](#) (NAP) makes no mention of cybersecurity or cyber/digital threats and includes only one reference to technology (in a footnote). [Australia's Cyber Security Strategy Action Plan \(2023–2030\)](#) lacks a gender focus, mentioning women and gender only once. Moreover, these terms were only referenced once in Australia's remarks to the UNSC Arria-Formula Meeting on Cyber Attacks on Critical Infrastructure in May 2023, despite the fact we are increasingly witnessing differentiated gendered impacts of cyber-attacks on critical infrastructure, especially healthcare.² Conversely, the first Progress Report on NAP implementation, published in 2024, contains no references to cybersecurity. However, examples of the cybersecurity-related work of NAP implementing agencies are beginning to emerge. They include Cyber Safety Pasifika, a joint regional initiative to reduce technology-facilitated gender-based violence (TfGBV), led by the Australian Federal Police (AFP); training and technical assistance by AFP to the Indonesian National Police's Women and Child Protection Unit; the Cyber and Critical Tech Cooperation Program, led by the Department of Foreign Affairs and Trade (DFAT); and a case study of the Women in International Security and Cyberspace Fellowship.³

This report does not aim to research all possible avenues of integration between the WPS Agenda and cybersecurity (see Box 1). Rather it will focus predominantly on the impact of gendered disinformation. This focus was chosen due to the relevance of gendered disinformation to other gendered cybersecurity issues, such as TfGBV.

Photo: Shutterstock



Box 1: A snapshot of cybersecurity issues and linkages with the WPS agenda

Characterising cyber and digital threats was an important first step in understanding how they affect women's participation in security and peacebuilding efforts. Discussions in the workshops (see Section 2) highlighted multiple issues related to women's participation and leadership in cybersecurity. Outlined below is a high-level snapshot of the key cyber issues that arose and how they relate to the four WPS pillars of participation, protection, prevention and relief & recovery.

Issue	Description	WPS linkages
Lack of representation of women in cybersecurity	Gender imbalance in the leadership of the private sector, particularly large tech companies, in senior policy making roles, cyber roles in militaries and in the police, and among those working on transnational crime	
Technology-facilitated GBV	UNFPA defines TfGBV as an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media against a person on the basis of gender. ^a Other similar terms that are used include online GBV, cyber violence against women and girls (CVAWG) and violence against women and girls (VAWG) in digital contexts.	 
Data breaches and cyber attacks on networks and critical infrastructure	Can be state-sponsored or carried out by non-state actors. Cyber attacks on critical infrastructure and subsequent data breaches have often targeted humanitarian and health infrastructure. Whilst data hacks might be indiscriminate, they affect people differently, with women often facing heightened risks due to the types of data released. A number of documented data breaches relating to health infrastructure have involved the release of data about abortion services access and other sexual and reproductive health services.	 
Internet shutdowns	Internet shutdowns are an intentional disruption of internet or electronic communications. They are often used by state actors to control the flow of information. ^b Whilst internet shutdowns can be broad in application, they often target and undermine peacebuilding and human rights' work and disrupt access to critical infrastructure like healthcare.	  
Digital surveillance	This includes monitoring movement and surveillance that exposes certain, specific groups of people to increased risk.	 

a. UNFPA (n.d.), '[Technology-Facilitated Gender-Based Violence: A Growing Threat](#)'

b. Access Now (n.d.), '[#KeepItOn: fighting internet shutdowns around the world](#)', date accessed 26 September 2025; D. Brown & A. Pytlak (2020), '[Why Gender Matters in International Cyber Security](#)', WILPF & APC.

Issue	Description	WPS linkages
Gendered disinformation	Disinformation used to target and silence women and gender-diverse voices. Can also be a form of TfGBV. These attacks are gendered in nature and impact, and reinforce prejudices, bias and structural and systemic barriers to gender equality. It seeks to not only attack individuals but broader, collective movements for gender equality.	
Gender divide in access to ICTs and control of the digital space	Globally, women access ICTs less than men (62% compared to 57%). Meaningful access to the internet is also influenced by geographical location, economic power, age, racial or ethnic origin, social and cultural norms, and education. For example, a household may have access to one mobile device, but women's use (including for how long, what they can access etc.) may be controlled by the male head of household. ^c	
Development of AI	The rapid development of AI has implications for many of the issues above – for example, from making it easier to create deep fakes which are used in image-based abuse, being used to create and spread mis/disinformation, to the very information AI is developed off and trained on which often replicates existing gender inequalities and biases.	

Key: Four pillars of the WPS agenda



Calls for increased participation of women at all levels of decision-making, including in national, regional and international institutions; in mechanisms for the prevention, management and resolution of conflict; in peace negotiations; in peace operations, as soldiers, police and civilians; and as Special Representatives of the UN Secretary General.



Calls specifically for the protection of women and girls from sexual and gender-based violence, including in emergency and humanitarian situations, such as in refugee camps.



Calls for improving intervention strategies in the prevention of violence against women, including by prosecuting those responsible for violations of international law; strengthening women's rights under national law; and supporting local women's peace initiatives and conflict resolution processes.



Calls for advancement of relief and recovery measures to address international crises through a gendered lens, including by respecting the civilian and humanitarian nature of refugee camps, and considering the needs of women and girls in the design of refugee camps and settlements^d

- c. ITU (2023), '[Bridging the gender divide](#),' November, date accessed 26 September 2025; D. Brown & A. Pytlak (2020), [Why Gender Matters in International Cyber Security](#), p.6
- d. UNOAU (n.d.), '[The Four Pillars of United Nations Security Council Resolution 1325](#),' date accessed 25 September 2025.

Background photo: Shutterstock

In her report to the UN General Assembly, Irene Khan, the UN Special Rapporteur on Freedom of Expression,⁴ defined gendered disinformation as:

a strategy to silence women and gender-diverse voices. It is also a form of online gender-based violence in some situations. [...] Gendered disinformation is gendered because it targets women and gender nonconforming individuals, because of the gendered nature of the attacks and their gendered impact, and, very importantly, because it reinforces prejudices, bias and structural and systemic barriers that stand in the way of gender equality and gender justice. Gendered disinformation has multiple aims: portraying women as weak, incompetent and sexualized objects, incapable of leadership; driving women and gender nonconforming persons out of public spaces and places of power; and silencing those who do not comply with gender norms. Gendered disinformation attacks not only individuals but also their collective struggles by seeking to delegitimize feminism and gender rights.⁵

Khan drew attention to the fact that across all regions of the world, women, girls and gender non-conforming persons are a major target of disinformation and restrictions on expression.⁶ She highlighted how gendered disinformation is on the rise and not only uses false information to harm women and girls, but reaffirms and entrenches ideas, biases and stereotypes about women to attack them and hold them back. She noted that women politicians, journalists and those who are prominent in civil society are often targeted.⁷ These contentions are supported by data from the United Nations Educational, Scientific and Cultural Organization (UNESCO) and the Inter-Parliamentary Union (IPU). In 2022, the International Center for Journalists (ICFJ) and UNESCO published a global study of online violence against women journalists showing that 73% of women journalists had been attacked online.⁸ In 2021, the IPU reported that 46% of women parliamentarians in Africa had experienced sexist online attacks during their mandate, with the figure rising to 58% of women parliamentarians in Europe experiencing online attacks.⁹ State-sponsored gendered disinformation has also been documented, with state actors using orchestrated online platforms to manipulate information on gender-related issues, including in the Philippines, Brazil, Hungary and Uganda.¹⁰

The WPS Agenda can be utilised to inform and expand initiatives that mitigate against cyber threats against women and girls. This report contributes to the growing evidence on the importance of integrating gender, peace and cybersecurity, with a particular focus on gendered disinformation, and identifies emerging opportunities and considerations for NAP implementing agencies. The researchers sought to engage with civil society and government in Australia on the topic of WPS and cybersecurity, with a focus on gendered disinformation, incorporating diverse voices, communities and subject matter experts, and to identify insights and key opportunities for NAP implementing agencies. The report maps out the areas in which the WPS Agenda can be applied to gendered disinformation, and informs key opportunities for integration.

This report has four sections:

- Section 1 (this section) introduces the report and key concepts
- Section 2 outlines the research methodology, including research questions, methods and limitations
- Section 3 examines the impacts of gendered disinformation on peace and security
- Section 4 outlines opportunities for Australian Government agencies to consider in NAP implementation.

2. RESEARCH METHODOLOGY

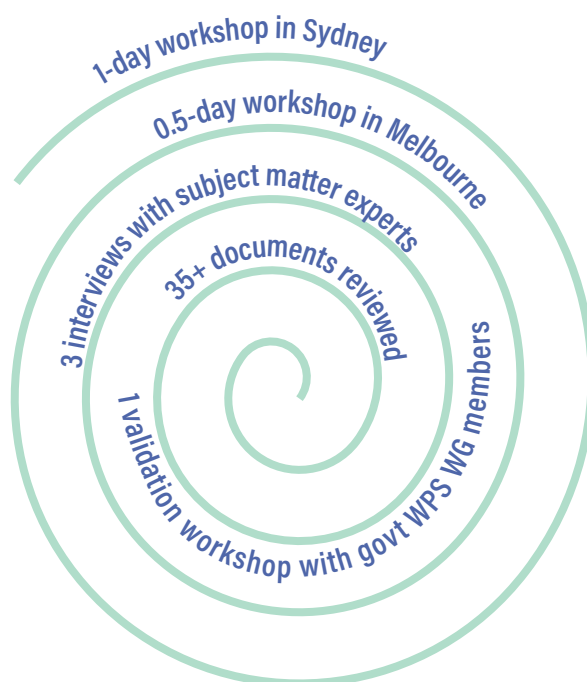
This research explored the intersection of the WPS Agenda and cybersecurity, with a specific focus on gendered disinformation. In particular, we sought to understand:

- 1. *What are the impacts of gendered disinformation on peace and security?*
- 2. *How can the WPS Agenda be applied to gendered disinformation cybersecurity threats?*

The research took a phased, qualitative approach, which involved a literature review, two workshops, key informant interviews with subject matter experts, and a validation session (Figure 1). The purpose of the **workshops** was to collectively and simultaneously consult with a diverse range of experts and practitioners on the links between cybersecurity and the WPS NAP. A full-day workshop was held in Sydney (4 June 2025) and a half-day workshop in Melbourne (14 August 2025). They included 54 participants from government, non-governmental organisations (NGOs), community-based organisations, consulting groups, the Red Cross Red Crescent (RCRC) Movement, networks, foundations, and universities. They were followed by **interviews** with three subject matter experts (August–September 2025) to triangulate and further unpack workshop data and fill gaps, with a particular focus on good practice examples and recommendations. Primary data collection was complemented by a **review of published evidence**. Findings were explored and tested in a **validation session** with members of the inter-governmental WPS working group, including representatives of DFAT, ACMC, Defence and Home Affairs.¹¹

Data analysis was conducted iteratively, with analysis from each phase informing the design of subsequent phases. Analysis of the data generated at the workshop in Sydney informed the design of the Melbourne workshop. Emerging findings were shared with Melbourne workshop participants in advance to inform and shape discussions. This avoided duplication and captured expertise more effectively than repeated linear discussions, allowing more in-depth development of findings. A similar approach was taken in the interviews with subject matter experts.

Figure 1: Research approach



Scope and limitations

Scope. Through the desk review and workshops, we identified a range of cyber issues relevant to the WPS Agenda and efforts to strengthen gender-sensitive approaches to peace and security – too many to cover meaningfully in this report. The research focused on gendered disinformation because of its relevance and consequences for gendered cybersecurity problems such as TfGBV. Gendered disinformation, especially in relation to TfGBV, can hinder the participation of women in public life in many ways.

The research focused on government and civil society. Private sector actors, particularly tech companies and social media platform owners, have important roles in relation to disinformation and cybersecurity. Consequently, Nonetheless, private sector representatives and experts were engaged through the workshops and interviews. However, the main purpose of the research was to identify opportunities for NAP implementing agencies, which are government bodies.

Stakeholder representation and availability. We intended the workshops to represent a diverse range of voices – from government, NGOs and community-based organisations, the RCRC Movement, universities and other organisations and individuals. However, the findings are not representative of all groups working on cybersecurity and/or WPS. Furthermore, workshops were held only in Melbourne and Sydney, so were not representative of all stakeholder groups across Australia. Participants were invited due to their involvement in disinformation, cybersecurity and WPS issues and/or their interest in sharing their experiences. Future work could include more online key informant interviews or focus group discussions to gather additional perspectives from locations across Australia and the broader Asia-Pacific region.

Photo: Shutterstock



3. UNDERSTANDING THE IMPACTS OF GENDERED DISINFORMATION ON PEACE AND SECURITY

There is growing recognition of the impact of gendered disinformation. Various organisations have documented the impact of online attacks on women politicians, journalists and human rights activists, including those focusing on communications, journalism and freedom of expression (Article 19, the Association for Progress Communications, Internews), global affairs (the National Democratic Institute for International Affairs (NDI), the Stimson Center) and gender equality and women's rights (UN Women, Women's International League for Peace and Freedom). This demonstrates how issues of cybersecurity, ICTs and mis/disinformation are cross-cutting and must be solved via collaboration across sectors and actors.

As noted earlier, Australia's NAP and its most recent Progress Report omit mis/disinformation, let alone gendered disinformation. This section outlines the impacts of gendered disinformation on peace and security with reference to the four outcome areas of the NAP to demonstrate its relevance and importance to NAP implementing agencies. The four outcome areas are:

- Reducing sexual and gender-based violence
- Supporting women's meaningful participation and needs in peace processes
- Supporting resilience, crisis, and security, law and justice efforts to meet the needs and rights of all women and girls
- Demonstrating leadership and accountability for WPS.



NAP outcome: Reducing sexual and gender-based violence

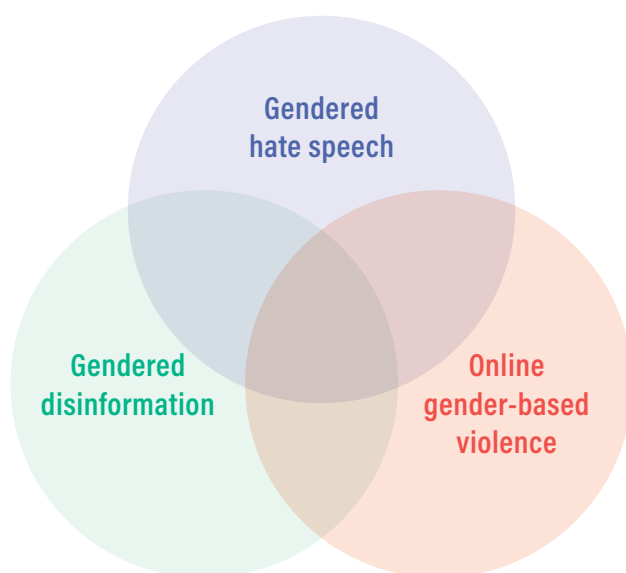
One of the four outcomes in Australia's NAP on WPS is to reduce sexual and gender-based violence, including combatting harmful gender norms, increasing women and girls' safety and security, and increasing access to justice. GBV is rooted in gender inequality and occurs in peaceful, fragile and conflict-affected contexts. In conflict and crisis-affected contexts, responses are often limited to extreme acts of violence, which overlooks the fact that all GBV violates human rights and requires attention. Furthermore, GBV can be a warning sign and symptom of conflict and therefore should not be considered separately from conflict prevention and resolution efforts – despite this traditionally being the case.¹² Over the last five years, there has been increased attention to the issue of TfGBV, yet it is still often considered less important than violence that occurs offline. Many police and other legal mechanisms lack the understanding or tools needed to combat TfGBV, leaving survivors and women's organisations without support.¹³

The Progress Report on NAP implementation demonstrated some examples of how understandings of GBV have been broadened to include TfGBV, and of efforts to strengthen the capacity of security and legal actors. For example, DFAT's Cyber and Critical Tech Cooperation Program has undertaken research to understand the prevalence, nature, and impacts of technology-facilitated domestic and family violence in Fiji, Tonga and Vanuatu (in partnership with Deakin University and WESNET). The program also involves working with local domestic and family violence support organisations to improve their identification and management of TfGBV.¹⁴ Capacity strengthening and technical

support efforts under the NAP include AFP's Cyber Safety Pasifika, which involved the co-design and co-delivery of training with Pacific stakeholders on combatting technology-enabled domestic violence for Pacific policing agencies (in partnership with WESNET) and technical assistance to the Indonesian National Police's Women and Child Protection Unit to improve cyber investigations of child exploitation and sexual and gender-based violence.¹⁵ Whilst these examples represent progress in inclusion of TfGBV under the NAP, gendered disinformation remains a blind spot.

Gendered disinformation, gendered hate speech and online GBV are separate but often overlapping issues (see Figure 2). The Economist Intelligence Unit (EIU) studied online violence against women and identified nine threat tactics, including mis/disinformation (used in 67% of cases analysed), cyber harassment (66%) and hate speech (65%).¹⁶ Online GBV is therefore much broader than gendered disinformation, but it is important to recognise that gendered disinformation can be a component. Conversely, threats of online violence are often part of gendered disinformation campaigns. Hate speech can include disinformation, and some gendered disinformation can advocate incitement to violence, hostility and discrimination, which can amount to hate speech. It is important to understand how these concepts interrelate in order to develop appropriate and tailored responses.¹⁷

Figure 2: Relationship between gendered, disinformation, online gender-based violence and gendered hate speech (adapted from the UN Special Rapporteur's report)¹⁸



Gendered disinformation can be a component of TfGBV, and online threats can translate into threats to physical safety. This contributes to the exclusion of women from public life and leadership roles.

In her report on gendered disinformation, the Special Rapporteur on Freedom of Expression noted that it can be harder to distinguish between disinformation, online threats and offline risks, which, alongside fear of reprisals, deters women from participating in peace processes and speaking publicly, including within UN forums.¹⁹ Others have documented how gendered disinformation and online threats can translate into threats to physical safety. In its 2020 study, the EIU found that 1 in 10 women surveyed experienced physical harm as a result of online threats.²⁰ A case study of gendered disinformation and online abuse against women in politics in India has noted that online hate and disinformation are used to target women in politics, particularly religious women. In 2018, this led to five UN Special Rapporteurs raising concerns about use of social media in Indian

politics and how it was being used against those critical of the government, citing a case where a female journalist had received death threats.²¹

All GBV violates human rights. As understandings of gendered disinformation and TfGBV evolve, it's important we recognise how they affect gender equality and women's meaningful participation in peace and security efforts (discussed in more depth below).



NAP outcome: Supporting women's meaningful participation and needs in peace processes

Australia's NAP on WPS aims to increase women's participation in conflict prevention and all peace processes. This aim is based on the recognition that women's participation in peace processes is often unequal, undervalued and unrecognised. When women are excluded from peace and stability processes, their needs and experiences are overlooked, entrenching inequality in post-conflict society. Furthermore, women face targeted violence, especially when politically active, intended to deter their participation in decision-making.²² The increase in use and accessibility of ICTs has – in many cases – provided opportunities for women to organise, advocate and participate in political processes, but also means that many women face threats, including TfGBV, online.

Women political leaders, journalists and human rights defenders are often targets of gendered disinformation, which has a silencing effect and deters women's participation in conflict prevention and peace. Internews and NDI have documented how gendered disinformation and cyber threats are used to intimidate, degrade and ultimately silence women leaders. In its submission to the UN Special Rapporteur on Violence Against Women, NDI noted how online harassment of women undermines their personal security in ways different to men. It contributes to women self-censoring and withdrawing from public life, which undermines democracy more broadly and has a chilling effect for others (discussed further below).²³ Internews also analysed the social media accounts of women leaders in India and found that the intention of cyber threats was to intimidate and discredit these women and silence them. In most cases it worked, with women choosing to withdraw from public life and/or online involvement. These findings are similar to those in other contexts, including Sierra Leone.²⁴ An IPU survey of 55 women legislators worldwide found that 81% had experienced psychological online GBV, including high incidences of humiliating or sexual images (often fake or doctored) being circulated.²⁵

Gendered disinformation undermines democracy and peacebuilding by deterring individuals, especially women, from engaging in peace, justice and civic/democratic processes. It has psychological, physical, social and economic effects on individuals, and affects society more broadly. Public discourse is diminished by the exclusion and self-censorship of women leaders, journalists and activists, suppressing the knowledge and experience that they can bring to inform policy and decision-making. Furthermore, it means other community members, especially young women, see these activities as risky.²⁶ For example, Plan International surveyed 26,000 adolescent girls and young women in 26 countries and found that misinformation and disinformation online restrict girls' activism: 1 in 4 girls reported lacking confidence to share their views, and 1 in 5 girls stopped engaging in politics or current affairs altogether.²⁷ Similarly, ICFJ and UNESCO's survey of over 700 women journalists found that 30% said they responded to online violence by self-censoring on social media, and the EIU's survey revealed half of women said they felt the internet was not a safe place to share their thoughts.²⁸ These examples demonstrate the flow-on effects of gendered disinformation and cyber-attacks on both individuals and society.

Gendered disinformation reduces social cohesion by undermining trust in women leaders.

Gendered disinformation exploits gender inequalities, stereotypes and prejudices, as well as other social divides, including racism, homophobia and transphobia. In research by ICFJ and UNESCO, Black, Indigenous, Jewish, Arab, Asian and gender-diverse journalists experienced both the highest rates and the most severe consequences of online violence.²⁹ LGBTQIA+ communities are also disproportionately affected, with research from 18 countries finding that a higher proportion of gender-nonconforming persons reported having lies spread about them (29%) than heterosexual persons (17%).³⁰ Other identity-related characteristics beyond race, ethnicity and religion may also feature in gendered disinformation. For example, women representatives of the deaf community in Colombia have been targeted with violent graphic interchange format (GIF) images and video clips that use sign language.³¹ Public shaming that results from the spread of gendered disinformation can also isolate individuals from family, work colleagues, neighbours and the broader community, weakening social networks and increasing the vulnerability of those affected.³²



NAP outcome: Supporting resilience, crisis, and security, law and justice efforts to meet the needs and rights of all women and girls

Under the NAP, Australia seeks to support resilience, crisis and security, law and justice efforts to meet the needs and rights of all women and girls. Historically, humanitarian, legal and security responses have failed to recognise or meet the specific needs of women and girls, resulting in inadequate protection, support and access to justice mechanisms during and after crises. This limits their involvement in and contributions to recovery and reconstruction.³³

Disinformation can hinder the work of humanitarian and security actors in crisis and conflict-affected contexts, and social media and other online platforms worsen this phenomenon. The 2018-20 Ebola epidemic in DRC highlighted the challenges of mis- and disinformation for humanitarian response and how it can spread both online and offline: only around 26% of people in North Kivu had internet access, yet mis/disinformation was able to spread rapidly from WhatsApp to communities offline.³⁴ Whilst there has been little attention to gendered disinformation in response and recovery settings, disinformation about sexual and reproductive health and rights (for example, the abortion referendum in Ireland) has had gendered impacts, showing that a gender lens is important.³⁵

Furthermore, states' responses to disinformation can have adverse effects and restrict freedom of expression. The UN Special Rapporteur highlighted how efforts to criminalise speech are increasingly being turned against women and women's rights activists. She cited examples from Pakistan (laws criminalising blasphemy were used to condemn the Aurat March ['Women's March']) and Indonesia (survivors of sexual violence who have spoken online about their experiences have been prosecuted for criminal defamation).³⁶ Instead, she argued states should regulate social media with respect to due diligence, impact assessment, transparency and accountability of companies. Her report also emphasises the importance of broader gender equality and anti-discrimination efforts to remove the exclusion, prejudices and stereotypes that gendered disinformation exploits. While states play a key role, private companies (who control social media platforms) must improve their content moderation, business models and process transparency.³⁷ Accordingly, efforts to support crisis response and recovery, and security, law and justice mechanisms under the NAP must not be gender blind and counter gendered disinformation without having a chilling effect.



NAP outcome: Demonstrating leadership and accountability for WPS

The fourth outcome under the NAP on WPS focuses on demonstrating leadership and accountability for WPS. Providing leadership and accountability to advance WPS remains central. On the 25th anniversary of the WPS agenda, we are seeing a retreat from gender equality, with states winding back diversity and inclusion efforts.³⁸ Without strong leadership and mechanisms to track progress, commitments to gender equality and women's rights in peace and security contexts risk being sidelined or implemented inadequately, especially given broader humanitarian and development funding cuts.

Outside of WPS, Australia has been demonstrating international leadership on the issue of online safety, especially for children.³⁹ The eSafety Commissioner's Office has also taken action against social media platforms to force removal of violent video material.⁴⁰ The eSafety Commissioner is also Australia's lead representative on the Global Partnership for Action on Gender-Based Online Harassment and Abuse (the Global Partnership), which brings together national governments, international organisations, the private sector and civil society organisations to study, reduce and prevent TfGBV. In 2024, the Global Partnership issued a statement to draw attention to the threat gendered disinformation represents to electoral integrity, access to information and the exercise of freedom of expression.⁴¹

As outlined above, gendered disinformation represents a serious threat to the safety of women, girls and gender-nonconforming individuals, which deters their participation in conflict prevention, resolution and peacebuilding. Australia can use its knowledge and expertise in online safety (particularly that of the eSafety Commissioner's Office) to advance the work of NAP implementing agencies on reducing gendered disinformation and other cyber hazards in the context of WPS. In addition, the Australian Government can bring together the private sector, women's rights organisations (WROs), women peacebuilders and the humanitarian and development sectors to facilitate learning and knowledge exchange.

4. EMERGING OPPORTUNITIES AND CONSIDERATIONS FOR NAP IMPLEMENTING AGENCIES

It is clear that gendered disinformation has a detrimental impact peace and security and making stronger linkages with the WPS agenda could help to address these challenges. This report now turns to opportunities and considerations for NAP implementing agencies to integrate efforts to address gendered disinformation into WPS NAP implementation. The options identified below are not exhaustive and will require further research and discussions with key interlocutors, as well as contextualisation to individual NAP agencies. Key areas listed below were identified in workshops and expanded upon through interviews and desk-based research.

Key: NAP Outcomes

-  Reducing sexual and gender-based violence
-  Supporting women's meaningful participation and needs in peace processes
-  Supporting resilience, crisis, and security, law and justice efforts to meet the needs and rights of all women and girls
-  Demonstrating leadership and accountability for WPS
-  Crosscutting

Relevant NAP outcomes	Key area	Recommendation
	Safeguard digital participation and public presence of women peacebuilders and leaders	Provide tailored support to women's organisations and peacebuilders to access digital tools, training, and justice mechanisms, leveraging both cyber-focused and existing programs ■ Provide tailored support to WROs and women peacebuilders to access information, resources and training on ICTs, good digital hygiene and understanding their rights are online and how to seek support and justice when those rights are not upheld. ■ Look for opportunities to provide support through existing programs in addition to cyber-focused programs ■ Integrate digital safety and resilience strategies into support for women mediators (including the Pacific and the Southeast Asian Women Peace Mediators Networks), leaders, activists, and human rights defenders ■ Establish digital security protocols and support systems for women participating in peace talks or civic dialogue (e.g. secure communications tools, access to digital literacy training, online moderation support) ■ Report transparently on progress, including through a dedicated reporting on WPS and cybersecurity in future NAP Progress Reports

Relevant NAP outcomes	Key area	Recommendation
	Strengthen internal digital resilience and safety through staff training and targeted support	Train staff in government and civil society organisations (e.g. humanitarian actors, I/NGOs) to spot and report misinformation and disinformation. This should be done alongside other efforts to improve digital and technology literacy of staff more broadly, including: ■ Embed mis/disinformation awareness in core staff training ■ Increase digital and technology literacy across agencies ■ Provide enhanced support to at-risk staff Provide tailored digital security support to public-facing staff at risk of gendered disinformation and other online threats
	Both deepen and elevate advocacy and leadership	Australia can convene different stakeholders, including government agencies and departments (such as the eSafety Commissioner's Office), women's and community-based organisations and the private sector to support knowledge exchange and learning ■ In doing so, Australia should look to leverage existing networks (e.g. The Global Partnership). ■ Allocate resources proportionate to private sector engagement, prioritising partnerships with companies demonstrating meaningful commitment ■ Leverage Australia's global role, such as through the eSafety Commissioner and regional partnerships, to advocate for integration of gender in multilateral cyber policy forums (e.g. OEWG, UN General Assembly debates) ■ Bridge the divide with tech platforms, digital tools and innovation to engage social media companies, messaging platforms and tech firms in codeveloping accountability and transparency mechanisms (e.g. flagging disinformation, labelling corrections, algorithmic adjustments) Support efforts to implement the UN Guiding Principles on Business and Human Rights. The Guiding Principles are designed to ensure social media companies exercise due diligence in corporate policies and support, rather than undermine, WPS outcomes.

Relevant NAP outcomes	Key area	Recommendation
 	Strengthen access to reliable, contextrelevant information in crisis settings by supporting media, WROs, journalists, and local communicators	Fund and support trusted local information actors that can boost transparency and accountability in times of conflict and disaster ■ Provide flexible, sustained funding to organisations like Internews, local journalists, WROs and community media so they can carry out factchecking, verification, and dissemination in crisis settings ■ Support training on crisis reporting, verification methods, digital security, disinformation detection, and resilient communications ■ Incentivise partnerships between WROs, media, tech platforms, and local networks to amplify credible voices Develop and support “information resilience” ecosystems at the community level ■ Work with local leaders, community influencers, women’s groups, and trusted intermediaries (churches, schools, elders) to map information networks (who people trust, what channels they use etc.) ■ Codesign “trusted packages” of messages, in local languages/formats, tailored to how communities receive information (radio, SMS, WhatsApp, loudspeaker, print) ■ Integrate early “prebunking” efforts — i.e. share common tactics of disinformation in advance, so communities are less susceptible when harmful narratives appear ■ Encourage media and information literacy (critical thinking, verifying sources) as part of humanitarian assistance packages Rapid response verification and counter-messaging capacity ■ Establish or support rapid verification hubs in crisis zones, which monitor disinformation trends in real time, flag emerging false narratives, and push corrective content ■ Create partnerships or funding lines for local factchecking units (with gender lens) to debunk disinformation that targets women, marginalised groups, or post-conflict reconciliation efforts Integrate information support into crisis programming and humanitarian response ■ Require humanitarian and peacebuilding projects (especially under the NAP) to include information and communications components — not as an afterthought but as core to protection, trust-building, and inclusion

Relevant NAP outcomes	Key area	Recommendation
	Super-charging regional collaboration	Expand joint initiatives on gender, peace, and cybersecurity by building on successful efforts and sharing lessons with regional government partners. The NAP Progress Report identified a number of joint initiatives with regional partners (e.g. led by AFP and DFAT). As cybersecurity continues to emerge as a new area for the WPS agenda, this work can be built upon and expanded (as appropriate, when demonstrated to be successful) to share learning with government partner agencies in the region ■ Review humanitarian crisis response frameworks to identify gaps in recognising and addressing gendered disinformation and its impacts ■ Collaborate with digital platforms and private sector actors to implement feminist principles in platform moderation, content regulation and transparency reporting—especially during elections or crises ■ Coordinate regionally with Pacific governments and civil society to address cross-border disinformation campaigns and TfGBV, using existing regional partnerships (e.g. Cyber Safety Pasifika) ■ Embed disinformation and digital harms into national and regional resilience strategies, ensuring they're not addressed only as ICT issues, but also as gendered peace and security concerns
	Engage diverse civil society expertise	More contextualised research is needed on online gendered disinformation that brings in a range of views. This includes understanding the impact of dis/misinformation in humanitarian settings and filling the data gaps that exist in low-income and middle-income countries ■ Embed meaningful consultation mechanisms with women peacebuilders, First Nations women, LGBTQIA+ communities, and gender-diverse tech experts in NAP implementation ■ Resource community-based research and pilot programs that explore gendered disinformation impacts in under-represented communities, particularly in the Pacific ■ Fund disaggregated data collection on digital harms, misinformation and peace and security participation, with a gender lens ■ Develop a shared WPS digital harms impact framework, with metrics to track disinformation's effect on women's participation, safety, and freedom of expression

ENDNOTES

- 1 ITU-T X.1205, [Overview of cybersecurity](#), date accessed 25 September 2025
- 2 Permanent Mission of Australia to the United Nations (2023), '[Statement delivered by H.E. The Hon Mitch Fifield, Ambassador and Permanent Representative, Australian Mission to the United Nations](#),' *UN Security Council Arria-Formula Meeting on Cyber Attacks on Critical Infrastructure*, 25 May.
- 3 DFAT (2024), [Australian National Action Plan on Women, Peace and Security 2021-2031 Progress Report](#), Australian Government.
- 4 Irene Khan's full title is 'UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression'.
- 5 Submission from APC cited in OHCHR (2023), [Gendered disinformation and its implications for the right to freedom of expression – Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression](#) (A/78/288), 7 August, pp.4-5
- 6 UN (2023), '[UN human rights expert warns of rise in 'gendered disinformation](#),' 23 October
- 7 Ibid.
- 8 J. Posetti, N. Aboulez, K. Bontcheva, J. Harrison & S. Waisbord (2022), [Online violence Against Women Journalists: A Global Snapshot of Incidence and Impacts](#), ICFJ & UNESCO
- 9 IPU & African Parliamentary Union (2021), [Sexism, Harassment and Violence against Women in Parliaments in Africa](#), pp.2-4
- 10 OHCHR (2023), *Gendered disinformation and its implications for the right to freedom of expression*, pp.16-18
- 11 AFP is also a member of the inter-governmental WPS working group but was an apology to the session.
- 12 UN Women (2015), [Preventing Conflict, Transforming Justice, Securing the Peace: A Global Study on the Implementation of United Nations Security Council resolution 1325](#), p.169; DFAT (2021), [Australian National Action Plan on Women, Peace and Security 2021-2031](#), Australian Government.
- 13 Interviews 1-3; L. Sharland & I. Dahir (2023), [Ending Violence Against Women and Girls in Digital Contexts: A Blueprint to Translate Multilateral Commitments Into Domestic Action](#), The Stimson Center, Washington D.C., USA.
- 14 DFAT (2024), *Australian NAP on WPS 2021-2031 Progress Report*, pp.26-27
- 15 Ibid, pp.26, 30
- 16 The nine threat tactics are: mis/disinformation, cyber harassment, hate speech, impersonation, astroturfing, violent threats, doxxing, video- and image-based abuse, and hacking and stalking. EIU (2021), [Measuring the prevalence of online violence against women](#), 1 March, date accessed 26 September 2025
- 17 OHCHR (2023), *Gendered disinformation and its implications for the right to freedom of expression*, pp.6-7
- 18 Adapted from OHCHR (2023), *Gendered disinformation and its implications for the right to freedom of expression*, p.6
- 19 OHCHR (2023), *Gendered disinformation and its implications for the right to freedom of expression*, p.11
- 20 EIU (2021), *Measuring the prevalence of online violence against women*
- 21 L. Di Meco (2023), [The Digital Mob and Its Enablers: Gendered Disinformation and Online Abuse Against Women in Politics in India](#), #ShePersisted, April, pp.12-13; The Wire (2019) '[UN Experts Concerned over Lack of Action on Death Threats to Journalist Swati Chaturvedi](#),' 18 February
- 22 UN Women (2015), *Preventing Conflict, Transforming Justice, Securing the Peace*; M. O'Reilly, A. Ó Súilleabháin & T. Paffenholz (2015), [Reimagining Peacemaking: Women's Roles in Peace Processes](#), International Peace Institute; DFAT (2021), *Australian NAP on WPS 2021-2031*
- 23 NDI (2018), [#NotTheCost: Stopping Violence Against Women in Politics](#), Submission by the National Democratic Institute to the United Nations Special Rapporteur on Violence Against Women, June, p.14

- 24 Internews (2023), [‘PIF Grantee Spotlight: Dr. Shilpi Jha on what it’s like researching online trolls and harassment targeting women in India,’](#) 19 July. See also Sierra Leone Association of Women in Journalism & Internews (2022), [Threats Against Public-Facing Women in Sierra Leone](#), December
- 25 IPU (2016), [Sexism, harassment and violence against women parliamentarians](#), October cited in D. Brown & A. Pytlak (2020), *Why Gender Matters in International Cyber Security*
- 26 OHCHR (2023), *Gendered disinformation and its implications for the right to freedom of expression*
- 27 Plan International (2021) [The Truth Gap: How misinformation and disinformation online affect the lives, learning and leadership of girls and young women](#), State of the World’s Girls Report, p.6
- 28 J. Posetti et al. (2022), *Online violence Against Women Journalists*, p.3; EIU (2021), *Measuring the prevalence of online violence against women*
- 29 J. Posetti & N. Shabbier (eds) (2021), [The Chilling: A global study of online violence against women journalists](#), ICFJ & UNESCO cited in OHCHR (2023) *Gendered disinformation and its implications for the right to freedom of expression*, p.9
- 30 Submission from the International Lesbian, Gay, Bisexual, Trans and Intersex Association and S. Dunn, T. Vaillancourt & H. Brittain (2023), [Special Report: Supporting Safer Digital Spaces](#), Centre for International Governance Innovation, p.38, both cited in OHCHR (2023), *Gendered disinformation and its implications for the right to freedom of expression*, p.9
- 31 NDI (2019), [Tweets that chill: Analyzing online violence against women in politics](#), p.22 cited in OHCHR (2023), *Gendered disinformation and its implications for the right to freedom of expression*, p.10
- 32 EIGE (2022), [Combating Cyber Violence against Women and Girls](#), Publications Office of the European Union; OHCHR (2023) *Gendered disinformation and its implications for the right to freedom of expression*,
- 33 UN Women (2015), *Preventing Conflict, Transforming Justice, Securing the Peace*; DFAT (2021), Australian NAP on WPS 2021-2031
- 34 V. Elliott (2020), [‘In Congo’s Ebola zone, misinformation persists even as cases slow,’](#) The New Humanitarian, 15 January.
- 35 OHCHR (2023) *Gendered disinformation and its implications for the right to freedom of expression*, (A/78/288), p.12
- 36 Ibid, p.15
- 37 Ibid
- 38 C. Harper, A. Khan, E. Browne, J. Michalko & E. Tant (2025), [‘There’s not enough money – so why spend it on gender equality and justice?’](#) ODI, 14 March
- 39 eSafety Commissioner (2025), [Learn about the Online Safety Act](#), Australian Government, last updated 28 August 2025, date accessed 29 September 2025; D. Speers, [‘Australia’s social media ban wins praise from Europe at UN event,’](#) ABC, 25 September 2025
- 40 T. Nair (2024), [‘The Australian eSafety Commissioner vs X: Testing the Effectiveness of Enforcement Powers on Platforms,’](#) *Australian Outlook*, Australian Institute of International Affairs, 20 May
- 41 eSafety Commissioner (2025), [‘Working with international forums and networks,’](#) Australian Government, last updated 18 March; Ministry for Foreign Affairs (2024), [‘Global Partnership Statement on Gendered Disinformation,’](#) Government of Sweden, 24 September

BIBLIOGRAPHY

- Access Now. '[#KeepItOn: Fighting Internet Shutdowns around the World.](#)' n.d. Accessed 26 September 2025.
- Article 19. '[Myanmar: Crackdown on Freedom of Expression with 24-Hour Monitoring.](#)' 1 April 2024.
- Brown, D., and A. Pytlak. [Why Gender Matters in International Cyber Security.](#) WILPF & APC, 2020.
- Carmo, A. '[Why Is the Manosphere on the Rise? UN Women Sounds the Alarm over Online Misogyny.](#)' *UN News*, 21 June 2025.
- Caster, M. '[Global Tech Companies' Deafening Silence on Deteriorating Internet Freedom in Hong Kong.](#)' *The Diplomat*, 29 February 2024.
- DFAT. [Australian National Action Plan on Women, Peace and Security 2021–2031.](#) Australian Government, 2021.
- DFAT. [Australian National Action Plan on Women, Peace and Security 2021–2031 Progress Report.](#) Australian Government, 2024.
- Di Meco, L. [The Digital Mob and Its Enablers: Gendered Disinformation and Online Abuse Against Women in Politics in India.](#) #ShePersisted, April 2023.
- European Institute for Gender Equality (EIGE). [Gender Equality and Youth: Opportunities and Risks of Digitalisation.](#) Publications Office of the European Union, 2019.
- EIGE. [Combating Cyber Violence against Women and Girls.](#) Publications Office of the European Union, 2022.
- EIGE. [Cyber Violence against Women and Girls: Key Terms and Concepts.](#) Publications Office of the European Union, 2022.
- EIGE. [Tackling Cyber Violence against Women and Girls: The Role of Digital Platforms.](#) Publications Office of the European Union, 2024.
- EIGE. [Combating Cyber Violence against Women and Girls: Developing an EU Measurement Framework – Methodological Report.](#) Publications Office of the European Union, 2025.
- EIU. '[Measuring the Prevalence of Online Violence Against Women.](#)' 1 March 2021. Accessed 26 September 2025.
- Elliott, V. '[In Congo's Ebola Zone, Misinformation Persists Even as Cases Slow.](#)' *The New Humanitarian*, 15 January 2020.
- eSafety Commissioner. '[Working with International Forums and Networks.](#)' Australian Government. Last updated 18 March 2025.
- eSafety Commissioner. '[Learn about the Online Safety Act.](#)' The Australian Government. Last updated 28 August 2025. Accessed 29 September 2025.
- Euronews. '[Myanmar Has Endured More Than a Month of Nightly Internet Shutdowns.](#)' 17 March 2021.
- Global Forum on Cyber Expertise (GFCE). '[Mainstreaming Gender in Cyber Capacity Building.](#)' Presented at the GFCE Annual Meeting 2022.
- GNET Research. '[Misogyny and Violent Extremism: Can Big Tech Fix the Glitch?](#)' 30 June 2025.

Harper, A., E. Khan, J. Browne, J. Michalko, and E. Tant. '[There's Not Enough Money – So Why Spend It on Gender Equality and Justice?](#)' ODI, 14 March 2025.

Htusan, E. '[Briefing: The Growing Emergency on Myanmar's Newest Battleground.](#)' *The New Humanitarian*, 18 February 2020.

Internews. '[PIF Grantee Spotlight: Dr. Shilpi Jha on What It's Like Researching Online Trolls and Harassment Targeting Women in India.](#)' 19 July 2023.

Internews. '[Five Challenges for Journalism.](#)' 9 October 2023.

IPU & African Parliamentary Union. '[Sexism, Harassment and Violence against Women in Parliaments in Africa.](#)' 2021.

International Telecommunication Union (ITU). '[Bridging the Gender Divide.](#)' November 2023. Accessed 26 September 2025.

ITU. '[ITU-T X.1205: Overview of Cybersecurity.](#)' n.d. Accessed 25 September 2025.

O'Reilly, M., Ó Súilleabháin, A., and Paffenholz, T. '[Reimagining Peacemaking: Women's Roles in Peace Processes.](#)' International Peace Institute, 2015.

Ministry for Foreign Affairs. '[Global Partnership Statement on Gendered Disinformation.](#)' Government of Sweden, 24 September 2024.

MOAS (Migrant Offshore Aid Station Foundation). '[The Impact of Misinformation and Disinformation on the Humanitarian Sector.](#)' 26 February 2024.

Nair, T. '[The Australian eSafety Commissioner vs X: Testing the Effectiveness of Enforcement Powers on Platforms.](#)' *Australian Outlook*, Australian Institute of International Affairs, 20 May 2024.

NDI. '[#NotTheCost: Stopping Violence Against Women in Politics.](#)' Submission to the UN Special Rapporteur on Violence Against Women, June 2018.

OHCHR. '[Gendered Disinformation and Its Implications for the Right to Freedom of Expression \(A/78/288\).](#)' 7 August 2023.

Open Net. '[Open Net publishes a shadow report on Indonesia digital rights to UN Human Rights Committee.](#)' 6 February 2024.

Pavlova, P. '[Confronting Gendered Harm in Cyberspace Is Not a Matter of Social Justice — It's a National Security Imperative.](#)' *Just Security*, 17 February 2025. Accessed February 27, 2025.

Permanent Mission of Australia to the United Nations. '[Statement Delivered by H.E. The Hon Mitch Fifield, Ambassador and Permanent Representative.](#)' UN Security Council Arria-Formula Meeting on Cyber Attacks on Critical Infrastructure, 25 May 2023.

Plan International. '[The Truth Gap: How Misinformation and Disinformation Online Affect the Lives, Learning and Leadership of Girls and Young Women.](#)' State of the World's Girls Report. 2021.

Posetti, J., Aboulez, N., Bontcheva, K., Harrison, J., and Waisbord, S. '[Online Violence Against Women Journalists: A Global Snapshot of Incidence and Impacts.](#)' ICFJ & UNESCO, 2022.

Rakhmetov, B., and Valeriano, B. '[The Consequences of Internet Shutdowns in Kazakhstan.](#)' *Council on Foreign Relations*, 24 February 2022.

- Sharland, L., Goussac, N., Currey, E., Feely, G., and O'Connor, S. [System Update: Towards a Women, Peace and Cybersecurity Agenda](#). Geneva: United Nations Institute for Disarmament Research (UNIDIR), 2024.
- Sharland, L., and Dahir, I. [Ending Violence Against Women and Girls in Digital Contexts: A Blueprint to Translate Multilateral Commitments Into Domestic Action](#). Washington D.C.: The Stimson Center, 2023.
- Sharma Punit, I. '[South Asia: The Real Cost of Internet Shutdowns](#).' *Rest of World*, 3 May 2022. Accessed 27 February 2025.
- Sierra Leone Association of Women in Journalism and Internews. [Threats Against Public-Facing Women in Sierra Leone](#). December 2022.
- Stimson Center. '[Gendered Disinformation: A National Security Threat](#).' 13 January 2025.
- The New Humanitarian. '[From Cyber Attacks to Bot Farms: The Top Tech Threats Humanitarians Face in Ukraine](#).' 9 March 2022.
- The Wire. '[UN Experts Concerned over Lack of Action on Death Threats to Journalist Swati Chaturvedi](#).' 18 February 2019.
- UN. '[UN Human Rights Expert Warns of Rise in 'Gendered Disinformation](#).'" 23 October 2023.
- UN Women. [Preventing Conflict, Transforming Justice, Securing the Peace: A Global Study on the Implementation of United Nations Security Council Resolution 1325](#). 2015.
- UN Women and UN University Institute in Macau. [Cybersecurity Threats, Vulnerabilities and Resilience Among Women Human Rights Defenders and Civil Society in South-East Asia](#), 2024.
- UNFPA. '[Technology-Facilitated Gender-Based Violence: A Growing Threat](#).' n.d.
- Xu, R. '[You Can't Handle the Truth: Misinformation and Humanitarian Action](#).' *ICRC Blog*, 15 January 2021.

ANNEX: ADVANCING THE WPS AGENDA IN CYBERSECURITY AND PROTECTION OF CIVILIANS WORKSHOPS

Australia's second NAP on WPS outlines how Australia will implement its commitments as part of UNSC resolution 1325 and the broader WPS Agenda. Humanitarian Advisory Group organised in-person workshops in Sydney and Melbourne to delve into two thematic issues relevant to the WPS Agenda, bringing together a range of groups, experts, thinkers and practitioners. Insights from the workshops and other activities during the year contributed to reports which provide recommendations for Australian Government implementing agencies to strengthen NAP implementation.

SYDNEY WORKSHOP PROGRAM

Day 1: Gender, Peace and Cybersecurity

Date: Wednesday 4 June 2025

Time: 9:00am – 4:30pm.

Venue: Sofitel Sydney Darling Harbour, 12 Darling Dr, Sydney NSW 2000

Day/Time	Session
08:30	Registration
09:00–09:30 (30 mins)	Welcome and Framing Acknowledgement of Country, welcome remarks, and an overview of workshop goals and structure.
09:30–10:30 (1 hour)	Keynote Panel: The Cybersecurity-WPS Nexus This session highlighted how cyber threats intersect with peace and security efforts in the region and undermine women's leadership in crises. It explored the complexities of mis- and disinformation as well as initiatives to counter cyber threats. Panellists ■ Valentina Baú, Co-Director of Western Sydney University Humanitarian and Development Research Initiative ■ Rafiq Copeland, Senior Technical Advisor, Internews ■ Myfanwy Wallwork, AI Governance Lead, Human Technology Institute, University of Technology Sydney Format: Moderated panel discussion followed by audience Q&A
10:30–11:00 (30 mins)	Morning Tea Networking and informal discussions

11:00–12:30 (1h 30m)	Expert Panel: Gendered Cyber Threats and Barriers to Participation This session focused on gendered cyber threats including how these impact on women's participation and leadership and gender-sensitive responses in digital conflict settings. Panellists ■ Ernez Dhondy, Acting CEO, YLab ■ Rachel Jin, Strategic Advisor, Fiji Truth and Reconciliation Commission ■ Hollie Johnston, Legal Adviser, International Humanitarian Law, Australian Red Cross Format: Moderated panel discussion followed by audience Q&A
12:30–13:30 (1 hour)	Lunch
13:30–15:00 (1h 30m)	Co-Design Workshop I: Diagnosing the Problem This session involved small, facilitated breakout groups to address the following questions: 1. How do cyber threats, such as online harassment, disinformation, and digital surveillance, impact women's participation in security and peacebuilding efforts in conflict-affected regions? 2. What are the key barriers to women's participation and leadership in cybersecurity and digital peacebuilding, and how can these be addressed within the WPS agenda? 3. How does the use of cyber tools in modern warfare and conflict influence women's roles and vulnerabilities in both physical and digital spaces? Groups were asked to map challenges using stakeholder perspectives (e.g., government, civil society, private sector, regional actors)
15:00–15:15 (15 mins)	Afternoon Tea
15:15–16:30 (1h 15m)	Co-Design Workshop II: Strategy Lab During this follow-up session, groups focused on developing practical, context-sensitive strategies and policy recommendations for: 1. Strengthening digital protection for women 2. Embedding WPS in cyber policy 3. Regional collaboration on digital peacebuilding

MELBOURNE WORKSHOP PROGRAM

Date: Thursday 14 June 2025

Time: 10am – 5pm

Venue: The Cluster, Level 20, 31 Queen Street, Melbourne VIC 3000

Time	Session
10:00–13:00 (3 hours)	Gender, peace and cybersecurity This session explored emerging cybersecurity issues including the development of emerging technologies, mis- and disinformation, AI and the use of autonomous weapons, and how these need to be considered in relation to the WPS Agenda. Panellists ■ Matilda Byrne, PhD Candidate, RMIT University ■ Dinesh Jayasuriya, Principal Engineer, Susmet ■ Irene Scott, Humanitarian and Development Consultant Format: Moderated panel discussion followed by audience Q&A and roundtable discussion <i>Morning tea break included</i>
13:00–14:00 (1 hour)	<i>Lunch break</i>
14:00–17:00 (3 hours)	The intersection of the WPS and Protection of Civilians Agendas This session explored how the WPS Agenda can support protection of civilians in crises, including the forthcoming Declaration for the Protection of Humanitarian Personnel, issues of humanitarian access, the role of philanthropic organisations and learning from diaspora groups to Australia’s approach to protecting civilians during conflict. Panellists ■ Helen Durham, CEO, RedR Australia ■ Denise Furnell, International Risk and Security Consultant ■ Louna Ghawi, Senior Manager, Fragomen; Board Member, Victorian Divisional Advisory Board, Australian Red Cross ■ Catherine Green, Head of Impact Missions (Urgent Challenges), Minderoo Foundation Format: Moderated panel discussion followed by audience Q&A and roundtable discussion <i>Afternoon tea break included</i>