

ARTIFICIAL INTELLIGENCE AND THE WOMEN, PEACE AND SECURITY AGENDA IN SOUTH-EAST ASIA

ACKNOWLEDGEMENTS

This report was written by a team led by Eleonore Fournier-Tombs, United Nations University Centre for Policy Research (UNU-CPR), composed of JeongHyun Lee, UNU Institute in Macau (UNU Macau); Min Yang, UNU Macau; and Preeti Raghunath, University of Monash in Malaysia.

Additionally, the team benefited from valuable advice and support from Jingbo Huang, Serge Stinckwich and Jaimee Stuart, from UNU Macau; and Gaëlle Demolis and Alexandra Håkansson Schmidt from the United Nations Entity for Gender Equality and the Empowerment of Women (UN Women) Regional Office for Asia and the Pacific.

This research project was undertaken as part of the UN Women Regional Office for Asia and the Pacific project, Women, Peace and Cybersecurity: Promoting Women's Peace and Security in the Digital World, with the generous support of the Government of Australia, under the Cyber and Critical Tech Cooperation Program (CCTCP) of the Department for Foreign Affairs and Trade (DFAT), and of the Government of the Republic of Korea.

Exploring the connections between the Women, Peace and Security Agenda and cybersecurity is a key component of UN Women's Regional Framework Towards Peaceful, Inclusive Societies: Advancing the Women, Peace and Security Agenda and Inclusive Governance in the Asia-Pacific Region (2023-2027).

© 2024 UN Women. All rights reserved.

Published by the UN Women Regional Office for Asia and the Pacific. https://doi.org/10.17605/OSF.IO/H38WZ

Disclaimer: The views expressed in this publication are those of the author(s) and do not necessarily represent the views of UN Women, the UNU Macau or the United Nations or any of its affiliated organizations.





ARTIFICIAL INTELLIGENCE AND THE WOMEN, PEACE AND SECURITY AGENDA IN SOUTH-EAST ASIA





Australian Government



TABLE OF CONTENTS

GLC	GLOSSARY	
EXE	ECUTIVE SUMMARY	8
1.	INTRODUCTION	10
	1.1. Conceptual framework	10
	1.2. WPS and Human Security	13
	1.3. The AI Landscape in South-East Asia	14
	1.4. Global Perspectives on AI and WPS	16
2.	METHODS	18
3.	FINDINGS	20
	3.1 Al for Peace	20
	3.1.1. DATA ANALYSIS AND FORECASTING FOR CONFLICT PREVENTION, RESPONSE AND RECOVERY3.1.2. APPLICATIONS DEVELOPED TO DIRECTLY SUPPORT PEACE EFFORTS	21 22
	3.2 Neutral Al	24
	 3.2.1. SOCIAL MEDIA PLATFORMS FOR WPS ADVOCACY 3.2.2. FILTER BUBBLES AND SHADOW-BANNING 3.2.3. THE EFFECTS OF GENERATIVE AI ON PEACE AND CONFLICT 3.2.4. ANONYMITY AND LACK OF ACCOUNTABILITY: THE PERFECT STORM 	24 26 28 29

	3.3 Al for Conflict	29
	3.3.1. GENDERED IMPLICATIONS OF AUTONOMOUS WEAPONS SYSTEMS 3.3.2. SURVEILLANCE OF WOMEN AND WOMEN'S HUMAN RIGHTS DEFENDERS	29 30
	3.4. Systemic risks: privacy and cybersecurity, technosolutionism and the digital divide	31
	3.5. Stakeholder understanding of AI and WPS linkages	32
	3.6. Summary of the effects of AI applications on the WPS agenda	33
4.	RECOMMENDATIONS	38
	NEX 1. THODOLOGY	45
	NEX 2. CIAL MEDIA ANALYSIS REPORT	51

GLOSSARY

Artificial intelligence (AI)	"An interdisciplinary field, usually regarded as a branch of computer science, dealing with models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning."		
Autonomous weapons systems	Weapons that have programmed target profiles but no or minimal human control and which may be out of communication with a central command for an amount of time.		
Bioiometrics	The use of AI to identify people through their physical or biological characteristics (e.g., fingerprints, iris patterns, DNA), using image recognition or other pattern recognition algorithms.		
Cyberbullying	The use of electronic communications to threaten or intimidate a person or organization.		
Cyberstalking	The repeated use of electronic communications to harass or frighten someone, or to clandestinely gather information about them for later use.		
Digital divide	The knowledge, capacity and access gaps between those who have access to information and communications technology and the Internet and those who do not. This can be a geographic and/or demographic gap, such as the digital divide between women and men in South Asia.		
Disinformation	False information that intentionally misleads, such as propaganda intended to influence elections or foster conflict.		
Doxxing	The search and publishing of personal information about someone online without their consent.		
Generative Al	A type of AI model that responds to user prompts to generate new outputs (e.g., text, images or videos) based on data that the models have been trained on.		
Geographic information systems	A computer system that uses and analyses geographically referenced information, such as satellite images.		

¹ ITU-T F.749.13 (06/2021) and ITU-T F.749.4 (06/2021), as detailed in the terms database, available at: <u>https://www.itu.int/br_tsb_terms/#?q=artificial%20intelligence§or=T,R&from=2002-10-25&to=2022-10-25&status=Recommended&page=1</u>

Machine learning	An AI subfield that updates its underlying algorithms, or 'learns', in order to improve accuracy.
Misinformation	False information that unintentionally misleads, such as inaccurate health recommendations.
Misogyny	Dislike of, contempt for, or ingrained prejudice against women.
Natural language processing and large language models	A subfield of AI and linguistics that is concerned with interpreting and generating language, such as speech or text.
Peacebuilding	Peacebuilding aims to reduce the risk of lapsing or relapsing into conflict by strengthening national capacities at all levels for conflict management and laying the foundation for sustainable peace and development. It is a complex, long-term process of creating the necessary conditions for sustainable peace. ²
Personally identifiable information	Features of data, such as name or address, that can be used to identify or locate a person.
Recommendation algorithm	An algorithm that is used to suggest personalized content to a user.
Social listening	The practice of using artificial intelligence to analyse social interactions, especially content posted on social media, to identify trends in ideas, hate speech, conflicts, or disinformation.
Women, Peace and Security agenda	Based on a resolution adopted in 2000 by the UN Security Council (UNSCR 1325) and a further nine resolutions, the Women, Peace and Security (WPS) agenda promotes women's full and equal representation and participation in all levels of peace processes and security efforts and addresses the many challenges that women face in situations of conflicts and crises. The WPS agenda is framed under four inter-connected pillars: participation and representation; prevention protection; and relief and recovery (see section 1.2).

2 United Nations (2022). Peacebuilding at the United Nations. Terminology Website Available from https://peacekeeping.un.org/en/terminology

EXECUTIVE SUMMARY

As the world grapples with ground-breaking advancements in the field of artificial intelligence (AI), concerns are being raised on their implications for international peace and security. The United Nations Secretary-General's New Agenda for Peace (2023) outlines the weaponization of emerging technologies, such as AI, as a key concern. Likewise, the United Nations Security Council held their first-ever debate on AI in the context of international security on 18 July 2023, recognizing its potential to accelerate progress for sustainable development, while warning of the detrimental effects that irresponsible use of such technologies could have for peace, security and human rights at large.

The global mainstreaming of AI technologies has had important impacts on women's security. While AI can be used for conflict prevention and peacebuilding purposes, it is used unequally across genders; women are more impacted than men by the digital divide. Al systems have also been shown to pose security risks to women, particularly in terms of online harms, dis- and misinformation and privacy. Irrespective of these disparities, gender considerations are often overlooked in dialogues on AI in the context of international security and other areas. Similarly, as South-East Asian countries begin to develop strategies and regulations for AI, they seldom consider the gendered risks that AI poses, risks that are frequently obfuscated under the technology's projected economic potential.

This report examines AI's opportunities and risks from a Women, Peace and Security (WPS) lens, with a focus on South-East Asia. To deepen the understanding of the different functions AI may fill in the context of peace and security, the report looks closely at three dimensions of the technology: i) AI for peace, ii) neutral AI and iii) AI for conflict. In relation to these dimensions, the report found the following:

Al for Peace Al technology is built for the purposes of responding to conflict or reducing the likelihood of future conflict.	 The use of AI can have many benefits to advancing gender-responsive peace as it carries the potential to enhance the effectiveness of conflict prevention, humanitarian and peacekeeping efforts through rapid data analysis and development of innovative tools to facilitate dialogue and provide support services. Potential benefits are dampened by intrinsic biases across AI-systems; emerging privacy and security concerns stemming from new technologies; and, the gender digital divide and other obstacles to women's leadership and meaningful participation in AI development and governance.
Neutral AI AI technology is built neither for peace nor conflict, but nevertheless can impact them.	 Neutral AI-powered technologies, such as social media and generative AI, can be harnessed to support gender-responsive peace efforts, notably by CSOs that use AI tools for communications and advocacy. Generative AI and and other automated recommendation- and decision-making processes tend to repurvey gender stereotypes and produce harmful content such as disinformation, reduring their positive potential to leverage WPS principles. These tools can, on the flip-side, also be used to produce harmful content at an exponential rate.
Al for Conflict The objective of the Al technology is to engage in physical or virtual conflict.	These technologies carry numerous risks peace and security, with serious ethical and gender-related implications. Concerns are raised from women's rights organisations on ethical and security implications of the increased use of automted weapons systems, and the use of facial recognition and other AI-technologies to surveil gender- and women's rights advocates

This research also found that gender biases across widely used AI-systems to constitute a significant obstacle to the positive usages of AI in the context of peace and security. The research therefore examines four types of gender biases in AI that must be addressed before the region can fully benefit from technological developments:

- > Discrimination, in which AI systems provide different outputs for women than for men, based only on their gender.
- Stereotyping, where AI systems produce outputs that promote an image of women as inferior, sexualized or hateful.
- Exclusion, in which women face ofteninsurmountable barriers to participation in the development and governance of AI or that inhibit their access to its benefits.
- Insecurity, in which AI systems threaten women's psychological or physical safety.

Understanding and mitigating these biases is an important step towards developing a safe, inclusive and trustworthy AI ecosystem.

The WPS agenda offers a holistic analytical and policy framework to better understand the risks and opportunities that AI systems carry for conflict prevention and peace efforts. The following priorities were identified as key steps towards ensuring a conflict-sensitive and gender-responsive approach to AI development and governance.

RECOMMENDATIONS:

- Mainstream WPS considerations in national, regional and global dialogues on AI governance, and vice versa.
- Support the design of inclusive, conflict-sensitive and gender-responsive AI by ensuring that women have equal opportunities to lead and meaningfully participate in said processes.
- 3. Map and conduct gender and human rights impact assessments of AI systems and draft policies and legislation, including those relevant to the advancements of peace and security.
- Raise awareness and strengthen capacities of key stakeholders on risks and opportunities of AI tools for gender-responsive conflict prevention and peace efforts.
- Leverage AI for hate-speech monitoring, factchecking and countering disinformation on social media, accounting for the use of misogynistic and otherwise harmful gendered narratives.
- 6. Strengthen accountability mechanisms for social media companies by enhancing users' agency in choice of providers and platforms, with specific attention to inclusive and rights-based solutions.





The rapid development of AI has recently dominated headlines, including its potential values and risks in the peace and security process. AI has been used to provide assistance in post-disaster recovery and to restore conflict-affected areas by optimizing the distribution of aid, evaluating building and soil damage, predicting migrant movement and much more. AI-powered tools, including social media and social media analysis, geographic information systems, data analytics and visualization, machine learning and natural language processing, all have the potential to set back or propel forward the WPS agenda, depending on the way in which they are used.

Ethical issues arising from the deployment of autonomous weapons and mass surveillance have sparked vigorous debates among relevant stakeholders. Other AI-related risks, such as privacy, digital propaganda, gender and racial biases, dis- and misinformation, have caused serious concern among peace actors. On 18 July 2023, the United Nations Security Council (UNSC) held its first-ever debate on AI. During the debate, Secretary-General António Guterres highlighted the potential of AI to identify patterns of violence, monitor ceasefires and strengthen peace and humanitarian efforts. He also raised a word of caution on how these technologies may be used with malicious intent to cause "death and destruction, widespread trauma and deep psychological damage at an unimaginable scale."³ Moreover, on 19 December 2023, the UNSC had an informal dialogue on artificial intelligence and its impact on hate-speech, disinformation and misinformation which explicitly and uniquely - sought to explore venues for AI to be used to support gender-responsive peace efforts and the implementation of the WPS agenda.⁴

Preventing the weaponization of emerging domains and promoting responsible innovation is also outlined as a priority action under the Secretary-General's New Agenda for Peace (2023), which highlights the enabling and disruptive potential of AI.⁵ Recognizing the importance of multilateral collaboration to govern rapid developments within the field, the Secretary-General also set up a High-level Advisory Body for Artificial Intelligence on 26 October 2023.

³ United Nations (2023). Secretary-General Urges Security Council to Ensure Transparency, Accountability, Oversight, in First Debate on Artificial Intelligence, SG/SM/21880, https:// press.un.org/en/2023/sgsm21880.doc.htm

⁴ UN Documents. Arria-formula meeting concept note: Artificial Intelligence: its impact on hate speech, disinformation and misinformation (posted on 19 December 2023). Accessible at <a href="https://www.securitycouncilreport.org/un-documents/document/arria-formula-meeting-concept-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its-impact-on-hate-speech-disinformation-note-artificial-intelligigence-its

⁵ United Nations (2023). Our Common Agenda Policy Brief 9 – A New Agenda for Peace, https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-new-agenda-for-peace-en.pdf

Risks and opportunities relating to AI were also addressed during the 67th Session of the Commission on the Status of Women (CSW67) in 2023. In its agreed conclusions, the Commission raised concerns over setbacks in gender equality caused by algorithmic bias, while describing how emerging technologies have facilitated new spaces for gender-based violence and discrimination. Nevertheless, the Commission also recognized the contributions of digitization in ensuring the "full, equal and meaningful participation and involvement of women in peace processes, conflict prevention, conflict resolution and peacebuilding", while stressing that women's leadership is paramount in preventing and eliminating conflictrelated gender-based violence that occurs though, or is amplified by, the use of technologies.⁶

While important strides are being made to better understand the impacts of AI on peace and security, these debates are still nascent and have yet to be considered within the WPS agenda.

Given the numerous applications and definitions of AI, it is important to have a solid common understanding of the scope of the technologies examined for this project. We therefore use the approach proposed by UNESCO in its Recommendations on the Ethics of Artificial Intelligence, which is to define AI as a set of technologies with two main subfields: machine learning and machine reasoning. This coincides with a more specific definition recently updated by the OECD: "An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that [can] influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment." 7

Areas of risk in AI have emerged in recent research and policy work, most notably codified in the EU AI Act first presented by the European Commission in April 2021. This document identified eight sectors considered high-risk: biometric identification: management and operation of critical infrastructure; education and training; employment; access to essential services; policing; migration, asylum, border management; and administration and of justice and democratic processes. While the European and global contexts are quite different from the South-East Asian one, there are significant commonalities in the applications of AI technologies which provide a starting point for this research.

In those high-risk areas, there are three categories of known risks to gender equality: **discrimination** (where algorithms have different outputs based on gender); **stereotyping** (where algorithms propagate specific and often undesirable gender norms); and **exclusion** (where women are not involved in development, leadership or policymaking around these technologies). To these we add **insecurity**, which can have both physical and virtual manifestations.

Although these risks are relevant to the WPS agenda, there is an additional focus on applications of AI that intersect with these high-risk sectors, but from a different perspective. Notably, we examine the ability of women to access these technologies for peacebuilding purposes, the impact of certain neutral applications on women's physical and psychological safety, and the effect and gendered risks of AI used for conflict.

With this framework in mind, AI applications of interest can be categorized as follows:

⁶ Commission on the Status of Women (2023). Sixty-seventh session – Innovation and technological change and education in the digital age for achieving gender equality and the empowerment of all girls: Agreed conclusions. E/CN.6/2023/L.3

⁷ OECD (2023). AI Principles Overview. Available from https://oecd.ai/en/ai-principles

TABLE 1. EXAMPLES OF AI APPLICATIONS IN A WPS CONTEXT

CATEGORY	AI APPLICATIONS
Peace: AI technology is built for the purposes of responding to conflict or reducing the likelihood of future conflict.	 Data analysis and forecasting for conflict prevention, response and recovery Early-warning and early-response systems Migration and human trafficking systems Monitoring for false information, misogynistic content and other harmful narratives Technology for peace ('peace tech') Deliberative AI for large-scale digital dialogues Chatbots providing legal and other support Mobile applications to support women CSOs and women's human rights defenders
Neutral: AI technology is built neither for peace nor conflict, but nevertheless can impact them	 Social media, news and search recommendation systems and filter bubbles Generative AI Misinformation content⁸
Conflict: the objective of the technology is to engage in physical or virtual conflict	 Autonomous weapons systems Disinformation content⁸ Surveillance without knowledge or consent (as in the case of women's human rights defenders)

.....

⁸ Here we distinguish between 'misinformation', unintentionally incorrect content, and 'disinformation', content intended to mislead. We also distinguish between AI systems used to create the content, such as natural language generation and image generation algorithms, and AI systems used to disseminate the content, such as social media recommendation systems.



agenda and **Human Security**

This research reflects a unique perspective in analysing the implications of AI to peace and security processes from a WPS lens. The WPS agenda is guided by a series of commitments to women's rights, including UN Security Council resolution 1325 (2000) adopted by the United Nations Security Council and nine supporting UN Security Council resolutions. Other key reference points include the 1995 Beijing Platform for Action and the 1979 Convention on the Elimination of All Forms of Discrimination against Women (CEDAW).

Enhancing women's engagement for sustainable peace requires an integrated approach that simultaneously addresses conflict prevention, resolution and recovery while strengthening national accountability and ensuring women's protection from all forms of human rights violations, including sexual and gender-based violence.

In the last two decades, the WPS framework has mainly focused on protecting women's rights in conflicts, including prevention of violence against women in conflict, increasing women's participation in all aspects of peace processes, and relieving the negative impact of conflicts on women. However, as the UNSCR 2242⁹ notes, the changing global context of peace and security poses new challenges for women and girls. These new issues include violent extremism, terrorism, refugee and displacement crises, climate change and the global health pandemic. These are increasingly intertwined with digital technologies, including emerging issues related to AI. However, cyber- and technologyrelated considerations have yet to be explicitly referenced in WPS resolutions.¹⁰

AI technologies are used around the world to support the realization of gender equality and women's rights goals in line with key WPS principles. For example, women-led organizations are starting to use AI-augmented tools to deliver life-saving services online, including psychosocial and judicial support. Women have used information and communications technology platforms, such as Facebook and WhatsApp, to disseminate educational materials and to call for joint action to advance peace processes. Notable examples from the region include young women from the Philippines using social media and digital tools to support female ex-combatants' reintegration into their communities and to mobilize support for the Bangsamoro Organic Law plebiscite, which was a milestone for the peace process in the Bangsamoro Autonomous Region of Muslim Mindanao (BARMM).¹¹

While the term *conflict* is commonly associated with armed confrontation, contemporary interpretations of the concept is spanning farther to account for social tensions caused by non-traditional conflict factors, such as climate change and the misappropriation of digital platforms. Similarly, changing global perspectives on peace are expanding the definition of peace beyond the absence of conflict to also include the presence of human security.

The United Nations identifies human security in terms of three pillars: freedom from fear, freedom from want and freedom to live in dignity.¹² Because this research includes the dynamics of women's security outside of conventional conflict, the freedom of fear pillar is particularly important. Donelly et al.¹³ have recognized the linkages between human security and WPS, explaining that WPS has implications beyond traditional concepts of conflict. In recent years, new areas of importance for women's security have included online safety and cybersecurity, both of which relate to AI technologies.

UNSC (2015). Resolution 2242. Available from http://unscr.com/en/resolutions/doc/2242

See Sharland, L., Goussac, N., Currey, E., Feely, G. and O'Connor, S. (2021). System Update: Towards a Women, Peace and Cybersecurity Agenda, United Nations Institute for Disarma-10 $ment \ Research \ (UNIDIR). \ Available \ from \ \underline{https://unidir.org/sites/default/files/2021-09/UNIDIR_System_Update.pdf$

GNWP and ICT4Peace (2021). Women, Peace, and Security and Human Rights in the Digital Age. Available from https://gnwp.org/wpcontent/uploads/PolicyBriefGNWP-2021c.pdf 11 United Nations Trust Fund for Human Security (2022). What is Human Security? Available from https://www.un.org/humansecurity/what-is-human-security/ 12

IPI Global Observatory (2021). Women, Peace, and What is Security. Available from https://theglobalobservatory.org/2021/10/women-peace-and-what-is-security/ 13

In the online world, virtual threats can come from a broader range of actors, including non-military groups and individuals. Online safety and cybersecurity span both conflict and non-conflict settings. This report considers main conventional and unconventional geographical areas of conflict in South-East Asia, some of which are long-standing and characterized by mass displacement, militarized responses, tensions in relation to territorial disputes and lack of sustainable peace processes (often without women's or civil society's participation).¹⁴

The ASEAN Regional Study on Women, Peace and Security¹⁵ observed challenges to women's security across the region, including:

- > Preventing and countering violent extremism.
- Impacts of pandemics on humanitarian and fragile settings.
- > Trafficking of people, drugs and arms.
- > Climate change and climate insecurity.
- > Mining and resource exploitation.
- > Cybersecurity and technology.

Present throughout these various dimensions of conflict and security are also threats that disproportionately affect women, notably domestic violence, sexual violence and hate speech, all of which can have both offline and online components. Considering the multiple challenges faced by women and girls, preventing all forms of discrimination, violence, health threats and social exclusion are, therefore, key components of women's peace and security. 01000010 01001100 01010011

1.3 The Al Landscape in South-East Asia

Many countries in South-East Asia are currently in the process of developing AI regulations. Several countries, such as Indonesia, Malaysia and Singapore, already have AI strategies that outline areas of government investment for AI growth. Others, such as Thailand, have adopted ethical frameworks that begin to address human rights and other safety concerns.¹⁶

The 2023 AI Readiness Index ranks all South-East Asian countries in terms of several dimensions of Al, including capacity, funding and governance (see Figure 1). Many countries achieve a higher score than the world average, while others, such as Myanmar, are lagging behind. On the situation in Myanmar, the use of social media to perpetrate violence against the Rohingya population has been highlighted by the United Nations.¹⁷ Algorithms used by social media platforms are said to have contributed to these widespread atrocities by allowing far-reaching spread of hateful content and amplifying disinformation content targeting Rohingya communities. Several United Nations Special Rapporteurs have also criticized the country's frequent use of Internet access restrictions and its targeted surveillance of pro-democracy activists since the February 2021 coup d'état.18

See also the 2022 Global Peace Index, which measures the peacefulness of countries. The Index is made up of 23 quantitative and qualitative indicators across three main domains: the level of societal safety and security; the extent of ongoing domestic and international conflict; and the degree of militarization. Available from <u>https://www.visionofhumani-</u>ty.org/wp-content/uploads/2022/06/GPI-2022-Briefing-web.pdf

¹⁵ ASEAN Secretariat, USAID and UN WOMEN (2021). ASEAN Regional Study on Women, Peace, and Security. Available from https://asean.org/book/asean-regional-study-on-wo-men-peace-and-security/

¹⁶ See also: Eleonore Fournier-Tombs, JeongHyun Lee, Arthtit Suriyawongkul, Preeti Raghunath, Matthew Dailey, Joyee Chatterjee, Philippe Doneys, Wanchanok Suthorn, Sirayuth Thongprasert, Kris Villanueva and Febroza Belda (2023). Gender-sensitive AI Policy in Southeast Asia. UNU Macau.

¹⁷ UN Human Rights Council (2018). Report of the independent international fact-finding mission on Myanmar, A/HRC/39/64

¹⁸ OHCHR (2022). Myanmar: UN experts condemn military's "digital dictatorship". Available from https://www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship



FIGURE 1. AI READINESS INDEX FOR SOUTH-EAST ASIAN COUNTRIES

Although AI development is still at an early stage, countries in the region have achieved rapid progress and have greatly benefited from widely harnessing it, particularly in the fields of finance, health, transport, education and public service. A recent study showed that AI could add almost \$1 trillion to gross domestic products across South-East Asia, with an additional \$366 billion in Indonesia.¹⁹ Regional government investments in AI have shown an increasing trend in recent years. Singapore, for example, will invest \$50 million to improve AI talent and double the number of AI apprenticeships over the next five years.²⁰

Several South-East Asian countries have formulated AI-relevant policies and national strategies, including Indonesia, Malaysia, the Philippines, Singapore, Thailand and Viet Nam.²¹ Although policy attention has been given to utilizing AI for economic development and public service delivery, little attention has been paid to this issue from a peace and security lens.

Moreover, despite advances in digital technology and Internet penetration across the region, there are still important differences in access to AI and Internet technologies, both between and within countries. As of 2021, 77 per cent of the population in the region is connected online. However, Internet penetration is much lower for those living in Laos, Myanmar and Timor-Leste.²²

The digital divide also exists along gender lines; women in South-East Asia are less likely than their male counterparts to contribute to technological development, own a mobile phone or access the Internet. Where data is available, women represent only between 20 and 40 per cent of the workforce in telecommunications and other information and communications technology activities in all

¹⁹ Kearney (2020). Al is integral to Southeast Asia's Future, but it is still at an early stage. Retrieved at: <u>https://www.kearney.com/digital/article/-/insights/racing-toward-the-futu-re-artificial-intelligence-in-southeast-asia</u>

²⁰ The Straits Times (2022). Singapore to invest \$71 million to attract, develop AI tech talent: DPM Heng. Available from https://www.straitstimes.com/business/singapore-to-invest-71-million-to-attract-develop-ai-tech-talent-dpm-heng

²¹ For example, the Indonesian government launched the National Strategy for AI (2020-2045), prioritizing AI solutions in areas such as health, agriculture, infrastructure, education and research, food security and public governance. Thailand has published both an AI strategy and AI ethics guidelines to support manufacturing, service industry, agriculture, research on science and technology. Singapore also incorporated ethical considerations in AI-relevant policies and strategies, with a particular focus on health, economic, technical, transport and public service purposes.

²² Tan, J.-E. (2021). Governance of Artificial Intelligence (AI) in Southeast Asia. EngageMedia. Available from <u>https://engagemedia.org/wp-content/uploads/2021/12/Engage_Report-Governance-of-Artificial-Intelligence-AI-in-Southeast-Asia_12202021.pdf</u>

ASEAN countries.²³ According to the International Telecommunication Union, only 61 per cent of women in the Asia Pacific region have access to mobile phones (compared to 72 percent of men), and 61 per cent of women have access to the Internet (compared to 68 per cent of men who do so). In lower-income countries in South-East Asia, such as Timor-Leste, women are even less likely to have access to any security benefits that might come from AI technologies.



1.4 Global Perspectives on AI and WPS

Globally, AI systems, especially those considered high-risk, pose four main threats to women: discrimination, stereotyping, exclusion and insecurity. Additionally, there is the threat of fostering violence, notably through active contributions to hate speech against women and minorities. This can be both an outcome of the aforementioned risks and a distinct threat in itself.

Discrimination in AI refers to the technology producing prejudiced outputs for certain groups based on their membership in that group. A notable example is the e-commerce company, Amazon's résumé screening application, which in 2018 was found to be filtering out women's résumés. Similarly, Apple co-founder Steve Wozniak highlighted that the AI system used for loan allocations through the Apple Card in the United States provided significantly higher loans to men than to women.²⁴ Common facial recognition software has also shown much higher error rates for women and people of colour compared to white men, attributed to imbalances in training datasets and insufficient testing.²⁵ While these instances are from the United States, these lessons reveal a legitimate concern that such discrimination could occur elsewhere, including in South-East Asia.

Al **stereotyping** often involves content-generation systems, such as those producing or interpreting images and text or recommendation systems that suggest videos, texts or images to Internet users based on user data-based profiling. There is substantial evidence of stereotyping in both content generation and recommendation systems, ranging from the sexualization of women, as documented by UNESCO,²⁶ to virtual assistants perpetuating "docile female" stereotypes. Notably, the X (formerly Twitter) chatbot Tay²⁷ generated thousands of misogynistic and racist messages before it was disabled.

Exclusion in AI refers to the inadequate representation of women in AI development and decision-making. This stems from the general underrepresentation and lack of recognition of women in technical fields, as well as limited access to funding and leadership opportunities in innovation. Exclusion in AI can have two effects on discrimination and stereotyping. It has been found that lower representation of women as developers can lead to discriminatory effects going unnoticed due to unbalanced training sets and inappropriate testing. Similarly, women developers and technology leaders have been shown to be less likely to allow the deployment of AI systems that propagate sexualization or violent gender stereotypes.

Insecurity relates to how AI tools can put women's physical safety and their personal privacy interests at risk. For example, a range of AI tools facilitates doxxing and other invasive activities, increasing the likelihood of direct physical attacks on them, their families or their property. This can be exacerbated by social media algorithms that are designed to elevate the visibility and spread of content that induces strong negative reactions, such as misogynistic speech.

Knight, W. (2019). The Apple Card Didn't 'See' Gender—and That's the Problem. Wired. <u>https://www.wired.com/story/the-apple-card-didnt-see-genderand-thats-the-problem/</u>
 Buolamwini, J., & Gebru, T. (2018). *Gender shades: Intersectional accuracy disparities in commercial gender classification*. Paper presented at the Conference on fairness, accountability and transparency.

²³ Marsan, G. A. (2021). Artificial Intelligence in Southeast Asia: Upskilling & Reskilling to Narrow Emerging Digital Divides in the Post-Pandemic Recovery.

²⁶ UNESCO and EQUALS Skills Coalition (2019). I'd blush if I could: closing gender divides in digital skills though education. Policy Paper.

²⁷ Neff, G. (2016). Talking to bots: Symbiotic agency and the case of Tay. International Journal of Communication.

More broadly, however, each one of the first three risks – discrimination, stereotyping and exclusion lead to women's insecurity. Discriminatory AI in areas such as employment, finance and service delivery can have significant, long-lasting socioeconomic impacts on women. In certain cases, discriminatory systems can have more direct effects on the security of women and gender non-conforming persons in cases where AI systems are applied to security contexts. For example, facial recognition systems used in migration management systems, which are less accurate for women, can affect their ability to move safely between borders, particularly in cases of forced migration.

Moreover, stereotyping in AI is directly linked to gender-based violence, as content that sexualizes or portrays violence against women correlates with increases in physical violence.²⁸ This is a significant concern in South-East Asia, where there is evidence that misogynistic content increased on social media during COVID-19.

There are several mechanisms by which AI can affect the spread of stereotyping content on social media. AI generation systems, such as GPT-4 (which generates text) and Midjourney (which generates images), tend to produce sexualising content, even when they are not asked to do so. Further, recent experiments even show examples of image-generating algorithms producing sexual images of children without being prompted.^{29,30,31} Additionally, some AI recommendation systems on social media are designed to intentionally amplify polarizing or extreme content, thereby promoting violent or misogynistic speech. This can have serious implications for stability and social cohesion across societies.

Al tools tend to be global in nature, and many tools used in South-East Asia were developed in the United States. Gender biases already present in these tools therefore risk being transplanted to a South-East Asian context. For example, current automated online content moderation systems on social media platforms are less likely to work for non-English speaking users and lack contextual sensitivity.³² In discussions with UN Women, CSOs in South-East Asia have encountered challenges in engaging with social media companies on moderation of harmful gendered content, stressing that statements which are considered harmful in local contexts might not be perceived as such by content moderators from the Global North, resulting in lacklustre moderation of this type of content.

South-East Asian countries are still in the early stages of AI regulation, which means that they do not yet have effective mechanisms to mitigate these risks. In order to be used safely for women, AI tools will need to be assessed much more carefully, particularly in light of gender-responsive security considerations.

²⁸ Council of Europe (n.d.) What causes gender-based violence? Available from https://www.coe.int/en/web/gender-matters/what-causes-gender-based-violence

²⁹ Brewster, J., Arvanitis, L. McKenzie, S. (2023). The Next Great Misinformation Superspreader: How ChatGPT Could Spread Toxic Misinformation at Unprecedented Scale. NewsGuard. Available from https://www.newsguardtech.com/misinformation-monitor/jan-2023/

³⁰ Hao, K (2021). An AI saw a cropped photo of AOC [Alexandria Ocasio-Cortez]. It autocompleted her wearing a bikini. MIT Technology Review. Available from https://www.technolo-gyreview.com/2021/01/29/1017065/ai-image-generation-is-racist-sexist/

Khari, J (2022). DALL-E creates incredible images – and biased ones you don't see. Wired. Available from https://www.wired.com/story/dall-e-2-ai-text-image-bias-social-media/
 Waldron, P. (2023). One-size-fits-all content moderation fails the Global South. Cornell Chronicle. Available from https://news.cornell.edu/stories/2023/04/one-size-fits-all-content-moderation-fails-global-south

2. METHODS

This research project aims to answer the following questions:

- In what ways can AI technologies be used to support gender-responsive or gender-transformative peacebuilding, including conflict prevention and promoting social cohesion in the region?
- 2. What are the risks and opportunities, from a gender perspective, to using these technologies to advance peacebuilding, including through the WPS agenda? How might AI technologies adversely affect women's rights and security in the region?
- 3. What methods (for instance, developing policies, capacities or strategies) might be employed to mitigate the risks of AI to women's rights and security?

A mixed methods approach was used to address these questions, consisting of a secondary literature review, social media analysis and key informant interviews across the region. Interview respondents were sampled directly based on their roles as AI and WPS stakeholders and their expertise in either AI or WPS. Selected respondents represented a diversity of perspectives across the region by country and by sector (e.g., academia, civil society and the private sector; see Table 3). In total, seven countries³³ in the region were represented through 18 semi-structured interviews (30 to 45 minutes each).

Study limitations include not every country in the region being represented in interviews, and some interviewees being unaware of the effects of AI on the WPS agenda (gender impact assessments of AI tools are not regularly conducted or publicly shared, and the AI-WPS nexus is relatively new).

The social media analysis was conducted by analysing the activity of CSOs dedicated to promoting the WPS agenda in Indonesia, the Philippines, Singapore and Thailand. We first identified 40 CSOs and examined their activity on Facebook, Instagram, LinkedIn and X. Of those, we selected 34 CSOs that actively participated in social media and studied 10 of their most relevant posts.³⁴

34 See the full Social Media Report in Annex B for further details on the analysis methodology.

³³ The countries represented in the interviews were: Brunei, Malaysia, Myanmar, Singapore, Thailand, Viet Nam and Timor-Leste.

The social media analysis addressed the following questions:

- Which AI-influenced social media tools were used by CSOs in South-East Asia to further implement the WPS agenda?
- How were these social media tools used in support of the WPS agenda at the national, regional and global levels?
- 3. What gendered challenges or issues on social media were addressed by these CSOs, and how?

A total of 238 social media posts from CSOs were extracted from the full sample of 340 according to the

following selection criteria: content that supported the WPS agenda; social media posts that showed relatively high interactivity with their followers in terms of number of comments and/or favourites and/or views; and the diversity of tools used (e.g. the captured posts were reposted on other social media platforms by each organization). Each post was then manually coded according to purpose and theme.

The overall research findings were validated during an online workshop held in May 2023. Feedback from these consultation activities was incorporated into the final findings.

Further details on research methods can be found in Annex A.



FIGURE 2. NUMBER OF INTERVIEWEES BY CATEGORY

3. FINDINGS

The findings from the research suggest that in each category of AI application (AI for Peace, Neutral AI and AI for Conflict), there are different degrees of favourable and unfavourable effects on genderresponsive peace and women's engagement in peace efforts. In analysing tools used in peace work and conflict settings, it is clear that when WPS principles are not accounted for, the tool tends to bear higher risks or even unfavourable effects for conflict- and gender-sensitivity across peace efforts. Tools mentioned by the interviewees as favourable included mobile applications designed to support women's safety and security.

In addition, interviewees' personal conceptions of both AI and the WPS varied widely, which impacted on how issues were interpreted. This divide made it more difficult to consider multistakeholder approaches to addressing AI and the WPS, which would require a common understanding of both themes from civil society, academics, government and international organisations and the private sector.



3.1 Al for Peace

Although AI can be used for peacebuilding purposes in many ways, even when the intention of the tools aligns with WPS values, there may still be some risks, especially when algorithmic biases are not properly addressed. Moreover, certain effects of digitization itself, such as cybersecurity risks, may particularly affect women, as women are more vulnerable to doxing attacks and stalking, which can have both online and offline repercussions. Finally, the digital divide means that marginalized women may not benefit from the positive effects of AI for peace.

This research shows that there are many uses of AI for peace that can support more gender-responsive peacebuilding, but significant technical and systemic risks and gaps need to be addressed for these benefits to be fully realized.

BOX 1. AI FOR PEACE

Definition:

AI technology is built for the purposes of responding to conflict or reducing the likelihood of future conflict.

Applications:

- > Data analysis and forecasting for conflict prevention, response and recovery
 - Early-warning and early-response systems
 - Migration and trafficking-in-persons systems
- > Applications developed to directly support peace efforts
 - Deliberative AI for large-scale digital dialogues
 - Fact-checking and countering disinformation
 - Chatbots providing legal and other support
 - Mobile applications to support women CSOs and women's human rights defenders

3.1.1. DATA ANALYSIS AND FORECASTING FOR **CONFLICT PREVENTION, RESPONSE AND RECOVERY**

Predictive analytical methods, notably those using machine learning, are increasingly being used in the context of conflict prevention, response and recovery measures. Automated data analysis can be used to rapidly detect patterns that predict looming escalation or eruption of violence. With more advanced AI-powered monitoring systems, peace and humanitarian actors will be able to respond to emerging needs more rapidly.

However, currently available predictive analysis tools for conflict prevention have nuanced effects; techniques that allow for the identification of relevant conflict risk factors carry ethical risks in predicting individual or group behaviour. As we will see below, preparing humanitarian or peacebuilding interventions as an outcome of forecasting can have positive results. However, predictive policing or intervention before crimes or violence are committed can be quite challenging, as they sometimes target people according to risk profile, which are known to have bias risks.

Early-warning and early-response systems

Early-warning and early-response systems are tools that help predict and prevent crises, including conflict and natural disasters. Although these systems can be qualitative in nature, they have increasingly incorporated AI-based predictive techniques, allowing for more comprehensive and rapid analysis. They can be used to anticipate conflict escalation and increased incidences of violence against women CSOs and women's human rights defenders. They can also either incorporate or exclude gender-responsive indicators, significantly affecting how disaster response is conducted. Since AI tools are useful only to the extent that they have been trained with appropriate data, improperly trained early warning systems will likely fail to flag issues critical to the WPS agenda.35

Early warning tools include social listening techniques to monitor misogynistic and other types of inflammatory content. AI can both create and disseminate misogynistic content. AI tools can be developed for content monitoring, notably to provide early warning of attacks against women CSOs and women's human rights defenders. Research conducted by UN Women in partnership with Monash University has found that there is a significant correlation between misogyny, the support of violence against women and the rise of violent extremism.³⁶ Detecting a rise in misogynistic content on social media platforms could forecast increased risks of radicalization and violence.

UN Women (2012). Gender-Responsive Early Warning: Overview and How-to Guide. Available from https://www.unwomen.org/sites/default/files/Headquarters/Attachments/ Sections/Library/Publications/2012/10/WPSsourcebook-04E-GenderResponsiveEarlyWarning-en.pdf Johnston, M. and True, J. (2019). Misogyny & Violent Extremism: Implications for Preventing Violent Extremism, Available from https://asiapacific.unwomen.org/en/digital-li-

³⁶ brary/publications/2019/10/misogyny-violent-extremism

A social enterprise, Mythos Labs, for example, has developed a tool called MIDAC, which aims to analyse fluctuations in the volume and content of online misogyny and hate speech. With the help of the tool, Mythos Lab was able to document the increase in online misogyny in Asia during the COVID-19 pandemic.³⁷ The tool has also been used to detect the spread of disinformation in conflict-affected areas.

The spread of disinformation and other types of harmful content often serves as a reflection of political shifts across societies, and hence acts as an important early warning indicator for conflict escalation or other shifts in public debate. With more comprehensive monitoring tools, such as big data analysis, trends across such narratives can be better identified and understood to inform appropriate responses.

Predictive policing techniques use analytics to predict and prevent crime. Though potentially effective, the use of such techniques raises ethical and regulatory questions.³⁸ India has used predictive policing in the context of violence against women. The technique involves the development of models that weigh different predictive factors for violence against women, most often in crime 'hot spots' and time of day, and occasionally individual characteristics of potential criminals. Police forces are then deployed to risk areas, and higher-risk individuals might be monitored more closely. There is less evidence of predictive policing techniques are being piloted in South-East Asia.

Migration and human trafficking systems

Al technologies are increasingly being used for migration management. Technologies include biometric identification for migrant tracking and border control, automated decision-making on individual cases, predictive analytics for humanitarian coordination, and remote sensing and image recognition to understand migration patterns. Migration management tools can be used to support humanitarian interventions more effectively for forced migrants, process visa cases more quickly and provide consistent identity tracking.

Globally, studies on AI in migration and gender have highlighted certain threats to women in relation to discrimination, privacy and cybersecurity.³⁹ For example, AI migration tools have been shown to be subject to gender biases that are commonly observed in AI systems. Research has also shown that facial recognition systems include entrenched gender- and racial biases, where women of colour constitute the group which faces the highest risk of being misclassified by such systems.⁴⁰ As a result, there are higher risks of error for women migrants, and the consequences of re-identification and privacy breaches can be considerable, as they can lead to both online and physical violence.⁴¹

3.1.2 APPLICATIONS DEVELOPED TO DIRECTLY SUPPORT PEACE EFFORTS

In South-East Asia, several AI tools are being piloted or deployed in a WPS context. These tools, implemented to enhance peacebuilding and response, include deliberative AI, chatbots and mobile applications.

Deliberative AI for large-scale digital dialogues

Deliberative AI tools for peace aim to facilitate virtual dialogues at scale so that large numbers of participants can engage on questions or converge on potential agreements. Features of these tools can include grouping contributions by topics, facilitating participant voting and, in more recent tools, suggesting modes of convergence or alternative proposals.⁴² Studies have shown how in other regions, these tools have been used on online platforms to facilitate public dialogue among government stakeholders, business leaders, civil society, and citizens at large, thereby facilitating

³⁷ Mythos Labs (2020). Researching the impact of COVID-19 on online misogyny in Asia. Available from https://mythoslabs.org/2020/08/06/researching-the-impact-of-covid-19-on-online-misogyny-in-asia/

³⁸ Davis, J., Purves, D., Gilbert, J., & Sturm, S. (2022). Five ethical challenges facing data-driven policing. Al and Ethics, 2(1), 185-198.

³⁹ Fournier-Tombs, E & Castets-Renard, C (2022). "Protecting vulnerable migrants against the risks of artificial intelligence technologies" In: The COVID-19 impacts on migration and migrants from a gender perspective. International Organisation for Migration (IOM).

⁴⁰ Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Paper presented at the Conference on fairness, accountability and transparency

⁴¹ Fournier-Tombs, E & Castets-Renard, C (2022). "Protecting vulnerable migrants against the risks of artificial intelligence technologies" In: The COVID-19 impacts on migration and migrants from a gender perspective. International Organisation for Migration (IOM).

⁴² The Computational Democracy Project (2023). Pol.is. Available from https://pol.is/home

public dialogue on an array of national issues and the crowdsourcing of laws.⁴³

AI-based language processing models have also been used to facilitate broad-scale mediation processes in other parts of the world. This includes initiatives that were implemented across Yemen and Libya in 2020 by the Innovation Cell of the UN Department of Political and Peacebuilding Affairs. Technology was used to hold real-time one-on-one dialogues with approximately 1,000 persons (30 per cent of which were women), taking stock of their views on key priorities for ongoing peace processes.⁴⁴ This example highlights the potential that strategically employed AI carries in ensuring that mediation processes are more inclusive, particularly of groups who face barriers in accessing traditional decisionmaking spaces, such as women, ethnic minorities and persons with diverse sexual orientation, gender identity, gender expression and sex characteristics.

Countering mis- and disinformation

Al can be used to create and widely disseminate false and misleading information. Conversely, it can also be used to detect manipulated content and track disinformation campaigns. As deepfakes (video, image or audio material of a person that has been digitally altered to appear to be someone else) grow more advanced, manipulated content will be more difficult to detect with the human eye. Al applications are currently being developed to detect subtle patterns of artificial manipulation that a human reviewer might overlook.

Similarly, Al's strong pattern recognition capacities may be used to detect the spread of disinformation by analysing the linguistic structure of content and cross-checking it with verified databases.⁴⁵ Hence, such technologies may be able to detect and tackle disinformation more effectively than humans can. This is an important component of conflict prevention and de-escalation efforts. However, such systems must be developed with consideration of gender- and context-specific factors in order to serve as effective tools for women peacebuilders and gender equality advocates.

Chatbots providing legal and other support

Increasingly, mobile applications are being developed with the intent to support women at large and women's human rights defenders. Many of these applications include AI-driven features, such as predictive elements, text generation and biometrics.

For example, mobile applications using generative AI and other types of algorithms⁴⁶ have been developed in the region to foster women's security. A striking example is Indonesia's BullyID tool,⁴⁷ which was developed to support victims of cyberbullying and harassment. In Thailand, the Sis Bot application⁴⁸ was created by a police investigator to provide immediate assistance to women experiencing domestic violence. Chatbot Rosa provides information to women experiencing violence in Timor Leste.⁴⁹ As women peacebuilders repeatedly report the toll that online harms are taking on their personal health and their ability to conduct their work, such applications fill an important function in safeguarding their mental health and physical safety.

Specific tools have also been developed to protect migrant workers from trafficking or poor labour conditions. For example, the APPRISE application, piloted in Thailand and since reworked in other South-East Asian countries, provides a way for workers to report issues to policymakers, and uses machine learning to detect patterns of exploitation.^{50,51} In other parts of the world, chatbots

⁴³ See for instance, MIT Technology Review (2018). The Simple but Ingenious System Taiwan uses to Crowdsource its Laws. Available from <u>https://www.technologyreview.</u> com/2018/08/21/240284/the-simple-but-ingenious-system-taiwan-uses-to-crowdsource-its-laws/

⁴⁴ Office of the Special Envoy for the Secretary-General for Yemen (2020). "Cutting-Edge Tech in the Service of Inclusive Peace in Yemen", Available from https://osesgy.unmissions.org/cutting-edge-tech-service-inclusive-peace-yemen; UN Secretary-General Annual Report on Women, Peace and Security 2021 (5/2021/827). Available from

org/cutting-edge-tech-service-inclusive-peace-yemen; UN Secretary-General Annual Report on Women, Peace and Security 2021 (S/2021/827). Available from 45 Helmus, T. C. (2022). "Artificial Intelligence, Deepfakes and Disinformation", RAND National Security Research Division, https://doi.org/10.7249/PEA1043-1

⁴⁶ Generative AI and recommendation algorithms are frequently used in chatbots and other types of information dissemination tools

⁴⁷ Pasaribu, A. (September 20, 2022). Bullying Indonesia. NAMATI. Retrieved at https://namati.org/network/organization/bully-id/

⁴⁸ UN Women (30 May 2019). Using Al in accessing justice for survivors of violence. Available from https://www.UN Women.org/en/news/stories/2019/5/feature-using-ai-in-accessing-justice-for-survivors-of-violenc

⁴⁹ UN Women Timor Leste (2018). "Rosa: an Innovative Chatbot to Report Sexual Harassment". Quarterly Newsletter October-December 2018.

⁵⁰ Thinyange, H. & Puthawong, M (2020). "Apprise: Using Al to unmask situations of forced labour and human trafficking. Rising Voices. Available from https://rising.globalvoices.org/ blog/2020/01/31/apprise-using-ai-to-unmask-situations-of-forced-labour-and-human-trafficking/

⁵¹ Thinyane, H., & Sassetti, F. (2020). Apprise: Sentinel surveillance of labor exploitation and its' potential impact on migration policy. In *Regional Integration and Migration Gover*nance in the Global South (pp. 239-259). Springer, Cham.

have been developed to provide legal support to protesters and human rights defenders who face judicial harassment due to their work.52

NEUTRAL AI 3.2.

This category of AI tools includes technologies built neither for peace nor conflict, but that nevertheless can impact them significantly. This category includes generative AI, which creates text, images and videos. The implications of these applications are illustrated in the case of the Myanmar conflict, where social media platforms were used to propagate hate speech related to the Rohingya group.53 In contrast, CSOs and humanitarian and human rights advocates have used Facebook⁵⁴, TikTok and X⁵⁵ to communicate with international organizations and with journalists highlighting ethnic violence and conditions in the Rohingya refugee camps. It must be noted that these platforms were not developed with conflictsensitivity or gender-responsiveness in mind, thus lacking policies and tools to adequately respond to harmful, inflammatory and escalatory content online, which risks undermining voices employing these platforms in a more positive manner.

BOX 2. NEUTRAL AI

Definition:

AI technology is built neither for peace nor conflict, but nevertheless can impact them.

Applications:

- > Social media, news and search recommendation systems and filter bubbles
- > Generative AI
- > Mis- and disinformation content

Social media and generative AI can be used to both support and undermine gender-responsive content. In neutral AI applications, the difference stems more from user intent than from technological errors. However, misconfigured algorithms in underlying social media can result in unintended acceleration of conflict and threats to the WPS agenda.

BOX 3. HOW IS AI USED IN SOCIAL MEDIA?

Social media platforms use AI algorithms in several ways, including recommendations, which rank and suggest content according to what the user is most likely to interact with; **content filtering**, such as capturing misinformation, hate speech or other banned content; and content generation, such as providing text content for social media bots or allowing users to generate their own text, images or videos to post. These algorithms have been promoting misogynistic content, filtering out gendertransformative and peace-promoting content and failing to filter misogynistic content. Many efforts have been made to address this, including tweaking the algorithms to reduce threats to women and educating social media users to use gender-promoting etiquette.

3.2.1. SOCIAL MEDIA PLATFORMS FOR WPS ADVOCACY

Social media platforms use several types of AI, primarily recommendation systems, which provide posts based on the predicted interests of an individual person (such as Facebook or X Feeds), and content generation systems, such as text or image creation algorithms. There is a tendency to associate

Asmolov, G. (2019). "Can Innovation Change the Balance of Power in Russia?", openDemocracy, Available from https://www.opendemocracy.net/en/odr/russia-protest-technology/. 52 United Nations Human Rights Council. (2018). Report of the detailed findings of the Independent International Fact-Finding Mission on Myanmar. Retrieved from https://www. 53 ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_CRP.2.pdf

Korineck, A. (2021). Why we need a new agency to regulate advanced artificial intelligence: Lessons on AI control from the Facebook Files. The Brookings Institute. Available from

https://www.brookings.edu/research/why-we-need-a-new-agency-to-regulate-advanced-artificial-intelligence-lessons-on-ai-control-from-the-facebook-files/ Myanmar has 1.2 million X users in 2021. DW (2021). "The battle for Myanmar plays out on Twitter, TikTok and Telegram". Available from https://www.dw.com/en/the-battle-for- 55 myanmar-plays-out-on-twitter-tiktok-and-telegram/a-57267075

Al-powered content generation systems with conflict and hate-speech, for example, to generate texts for social media bots or to create fake images for the propagation of disinformation. However, there is significant global evidence of women using Al-powered tools to create safe spaces, combat violence, prevent conflict and foster a peaceful culture.

Women peacebuilders in South-East Asia creatively use platforms such as Facebook, Signal and WhatsApp to expand their communication networks, share information about threats and violence, organize discussions on peacebuilding and analyze levels of violence in their communities. In the Philippines, for example, young women organized massive social media campaigns to encourage young people to vote and support the Bangsamoro Organic Law, which formally established the Bangsamoro Government as institutionalized by the peace agreement between the Government of the Philippines and the Moro Islamic Liberation Front.⁵⁶ CSOs have also used social media platforms to promote the WPS agenda more broadly. In a social media study conducted under the scope of this research,⁵⁷ it was found that a wide range of usage of these platforms, from awareness raising to fundraising. Consistent with WPS principles, the sampled CSOs focused not only on WPS agenda implementation in their own countries, but also raised awareness on these platforms on the peace work of other CSOs and women's rights issues in other South-East Asian countries and globally.

Furthermore, although Facebook remained the most popular social media tool, as reported in other research and in interviews, CSOs diversified their use of social media and typically used more than one tool to share their objectives. The CSOs also promoted uses of AI that would advance the WPS agenda, such as apps designed to promote women's safety.

Figures 3 and 4 present the types of goals that the CSOs aimed to achieve through their social media posts, as well as the WPS themes that the posts focused on.



FIGURE 3. OBJECTIVES OF CSO USE OF SOCIAL MEDIA FOR THE WPS AGENDA⁵⁸

⁵⁶ GNWP and ICT4Peace (2021). Women, Peace, and Security and Human Rights in the Digital Age. Available from https://gnwp.org/wpcontent/uploads/PolicyBriefGNWP-2021c.pdf 57 See Annex B for a full report on the findings of the social media analysis.

See Annex B for a full report on the findings of the social media analysis.
 Here, we differentiate between calls for participation and calls for action. The former refers to invitations to events and other activities organized by CSOs; the latter asks the audience to take specific steps, such as donating to support peacebuilding efforts.

FIGURE 4. CONTENT CATEGORIES OF CSO POSTS



There are several implications to this study. CSOs use social media tools to advance the WPS agenda and would use other AI-powered tools if available. There is also an opportunity for CSOs to increase their engagement with AI for social media. There may also be potential for CSOs to harness generative AI tools to create WPS content. Some of the useful functionalities of these tools include language translation, writing longer blogs or social media posts from short prompts, and writing communications or fundraising strategies.

While social media platforms serve as important contemporary peacebuilding tools, numerous women's rights and digital rights organizations have raised concerns regarding the negative implications that biased algorithms have on content moderation and other types of protection mechanisms.

3.2.2. FILTER BUBBLES AND SHADOW-BANNING

Social media uses algorithms in different contentfiltering contexts. In one context, an algorithm provides relevant content to users by ranking and recommending content for a home page or other type of feed. Another context is for monitoring and removing content that could be hateful, violent, overly sexualized or otherwise inappropriate. It is very difficult for individual users or organizations to know how these algorithms are affecting the content they view, due to lack of transparency across these algorithms. These two core uses have been shown to present risks for gender-responsive peace efforts when improperly implemented.

The phenomenon of 'filter bubbles' occurs when certain content is only shared with certain groups of people. This may limit the reach of genderresponsive and peaceful content, for example, to social media users who are already favourable to the content. Similarly, filter bubbles carry the risk of accelerating hateful, radicalising and misogynistic content. One example of this includes the emergence of 'incel culture', which stands on a foundation of misogynistic norms and support for violence against women. Nevertheless, there is some research suggesting that filter bubbles, when intentional, could enhance women's safety online by providing them with closed spaces.⁵⁹

'Shadow banning' can occur when AI tools used for content moderation do not display content from a user to their followers, generally without the knowledge of the user. It is difficult for someone to know if they have been shadow banned. Research has shown that this often occurs for content shared to promote gender equality and women's health and safety. Fowler documents numerous ways in which shadow banning can occur, notably when politically sensitive content is shared. Users who become shadow-banned may notice a reduction in social media traffic but would not otherwise be alerted by the platform ⁶⁰

The primary focus of secondary literature and interviewees' impressions on the risks of AI to WPS in the region is related to social media platforms. The adverse effects of social media platforms as tools for the propagation of disinformation and fostering conflict are well documented, notably in Myanmar (see Box 4).⁶¹

BOX 4. ONLINE DISINFORMATION IN MYANMAR

The gender dimensions of social media-based disinformation campaigns in Myanmar have not been extensively researched, as much of the analysis has focused on the exclusion of ethnic and religious groups. While there has been much more awareness in South-East Asia and globally about the non-neutrality of AI, the gender dimension appears more likely to be examined in a human security context than a conflict context. Nevertheless, alarms have been raised about misogynistic violence on social media in Myanmar, as documented by several UN-appointed experts.⁶²

Myanmar is experiencing the most violent conflict in the region; millions of Rohingya have fled the country due to a civil war between different groups and militias across the country. The contributions of social media platforms to the serious violations of international law have been extensively documented, notably in a United Nations special report on violations through social media platforms published in 2018.⁶³

The report criticized platforms for the polarizing forces of their algorithms, which encouraged content with shock value to be shared; the lack of monitoring of hate speech and disinformation, specifically in local languages (including many of the languages spoken by minority ethnic groups in Myanmar); and a lack of Myanmese employees in the social media companies. However, little analysis was done on the gendered impact of social media algorithms or other forms of AI tools. Nevertheless, there have been reports, corroborated by interviewees of this study, that gendered online content was rampant in the lead-up to conflict escalation.

For example, images and videos related to gender-based violence fuelled the conflict and incited further violence. Hateful disinformation was spread online that accused the Rohingya of being violent towards non-Rohingya women, thus framing

⁵⁹ Akane Kanai & Caitlin McGrane (2021) Feminist filter bubbles: ambivalence, vigilance and labour, Information, Communication & Society, 24:15, 2307-2322, DOI: 10.1080/1369118X.2020.1760916

⁶⁰ Fowler, G (2022). Shadow banning is real: Here's how you end up muted on social media. The Washington Post. Available from https://www.washingtonpost.com/technolo-gy/2022/12/27/shadowban/

⁶¹ See, for example: Fink, C. (2018). Dangerous speech, anti-Muslim violence, and Facebook in Myanmar. Journal of International Affairs, 71(1.5), 43-52.

⁶² United Nations (2023). Myanmar: Social media companies urged to stand up to junta. Press Release. Available from https://newsletter&utm_campaign=fd415b954c-EMAIL_CAMPAIGN_2023_03_13_04_24&utm_medium=email&utm_term=0_fdbf1af6o6-fd415b954c%5BLIST_EMAIL_ID%5D

⁶³ United Nations Human Rights Council. (2018). Report of the detailed findings of the Independent International Fact-Finding Mission on Myanmar. Available from https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_CRP.2.pdf

violations against the Rohingya as an effort to save non-Rohingya women. Interviewees for this research and other secondary reports corroborated the assertion that rumours on social media about Muslim men harming women fostered violent sentiments about the Rohingya.

As one respondent said, "There used to be rumours on social media about violence against women, which then led to violence on the ground against Muslims. People found it difficult to debunk because the hacking and looting had already started."

There are indications that polarizing stereotypes about women and Muslim men were accelerated by social media algorithms, fuelling the conflict. In turn, women and girls bore the brunt of this violence, even though, paradoxically, some of the conflict was fanned by outrage against violence *against* women.

There are two types of algorithms at play here. The recommendation algorithms tend to favour polarizing comments, such as comments about sexual violence. The content generation algorithms and bots, which are more recent, have, in many cases, been reported to generate inflammatory speech and create sexualized images of women.

3.2.3. THE EFFECTS OF GENERATIVE AI ON PEACE AND CONFLICT

The field of generative AI has advanced significantly since 2021. Tools enabling the general public to create

text, images and videos have been made widely available without consideration of their implications for gender or national or international security. Generative AI has benefited from the publishing of large language models such as ChatGPT, which allow users to request text that can be calibrated for tone, values and format. Generative AI poses the risk of accelerating disinformation by facilitating the rapid creation of authentic-seeming content at scale. It also makes it very easy to create convincing social media bots that intentionally share polarizing, hateful and misogynistic content.⁶⁴ In a study examining ChatGPT and misinformation, researchers found that when provided with 100 false narratives, the chatbot made false claims 80 per cent of the time.⁶⁵

Image-generating AI systems have been shown to easily produce misogynistic content, including creating sexualized bodies for women based on profile pictures⁶⁶ or images of people performing certain activities based on sexist and racist stereotypes.⁶⁷ Furthermore, these technologies have enabled the easy and convincing creation of deepfake videos, where false videos can be created of anyone based only on photo references. This has caused significant concerns for women, who might be shown, for example, in fake sexualized videos against their consent, incurring lifelong reputational and safety-related repercussions. There are notable examples from South-East Asia where women public figures have disengaged from their work, having been targeted by such deep-fakes and slander campaigns. Although researchers have been warning of the risks of deepfake pornography or extremist content in South-East Asia and globally for several years,⁶⁸ recent developments in AI are increasing the severity of the problem.

Lastly, deepfakes have also been used to manipulate content to mislead and inflame public debates and to spread disinformation in armed conflict settings.

⁶⁴ Deshpande, A., Murahari, V.S., Rajpurohit, T., Kalyan, A., & Narasimhan, K. (2023). Toxicity in ChatGPT: Analyzing Persona-assigned Language Models.

⁶⁵ Brewster, J., Arvanitis, L. McKenzie, S. (2023). The Next Great Misinformation Superspreader: How ChatGPT Could Spread Toxic Misinformation At Unprecedented Scale. NewsGuard. Available from https://www.newsguardtech.com/misinformation-monitor/jan-2023/

⁶⁶ Hao, K (2021). An AI saw a cropped photo of US Congresswomen Alexandria Ocasio-Cortez (AOC). It autocompleted her wearing a bikini. MIT Technology Review. Available from https://www.technologyreview.com/2021/01/29/1017065/ai-image-generation-is-racist-sexist/

Khari, J (2022). DALL-E creates incredible images – and biased ones you don't see. Wired. Available from https://www.wired.com/story/dall-e-2-ai-text-image-bias-social-media/68
 Biana, H. T. (2023). Mapping Uncharted Pathways in Contemporary Women's Studies. *Journal of International Women's Studies, 25(2), 1.*

3.2.4. ANONYMITY AND LACK OF ACCOUNTABILITY: THE PERFECT STORM

Several researchers have reported an uptick in online violence against women in the last few years. The COVID-19 pandemic has been raised as a cause, as it led to a perfect storm of closer proximity with family members due to shutdowns and travel restrictions, increased social media activity and general frustration and economic anxiety.⁶⁹

Two social media platform traits were raised as contributing factors: participant anonymity and the monopoly of platform providers. A considerable amount of online harassment and targeting is perpetrated by anonymous participants who have no fear of repercussions. While women could be easily identified and targeted, their attackers could stay hidden. Further, because the main online platforms monopolize the social media market, there was little to be done when they failed to moderate harmful content. As explained by one respondent, social media "became the Internet, searching was about searching for something in the social network...It was a feed-based ecosystem controlled by [a social media company] which doesn't have an office or people working there", while stressing that access to social media complaint mechanisms remains a challenge for women and civil society.



Al technologies are being developed in the context of conflict and defence operations, notably as autonomous weapons systems. They are also being increasingly used in the region to monitor activists, especially if they are part of a minority engaged in conflict with the state or neighbouring states. The technologies used include facial recognition, social media analysis and trend analysis using multiple data sources. Both Reuters⁷⁰ and Root⁷¹ have recently reported these trends across the South-East Asian region.

BOX 5. AI FOR CONFLICT

Definition:

Al technology is built to engage in physical or virtual conflict.

Applications:

- > Autonomous weapons systems
- Disinformation content (including that generated by Violent Extremist Groups and other malicious actors)
- Surveillance without knowledge or consent (as in the case of human rights defenders)

3.3.1. GENDERED IMPLICATIONS OF AUTONOMOUS WEAPONS SYSTEMS

The international community has expressed increasing concern regarding the development of autonomous weapons systems. However, this concern has paid limited attention to the gendered implications of the technology. As the 2022 Secretary-General Annual Report on WPS pointed out, "increasing autonomy in weapon systems are posing new challenges, which are rarely discussed or handled with sufficient gender analysis."⁷²

Autonomous weapons systems using AI can take many shapes, including robots, driverless tanks and drones. What they have in common is that they

⁶⁹ See, for example: UN Women (2022). The Shadow Pandemic: Violence Against Women during Covid-19. Available from https://www.unwomen.org/en/news/in-focus

⁷⁰ Chandran, R. (2022). Activists fear rising surveillance from digital silk road. Reuters. Available from <u>https://www.reuters.com/article/china-southeast-asia-surveillance-idUSL-8N1WDoDP</u>

⁷¹ Root, R. (2022). Digital rights activists in Southeast Asia increasingly at risk. Devex. Available from https://www.devex.com/news/digital-rights-activists-in-southeast-asia-increasingly-at-risk-103946

⁷² United Nations Secretary-General 2022 Annual Report on Women, Peace and Security (S/2022/740). Available from https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S-2022-740.pdf

are programmed to strike, usually using a target profile. This means that typically, no person controls exactly who, when and where they should strike. Rather, the automated weapons systems determine when to shoot based on parameters that have been programmed ahead of time.⁷³ These weapons are certainly concerning to all, regardless of gender, but some CSOs have proposed a gender-based approach to understanding specific automated weapons systems threats.

For example, Acheson has argued that automated weapons systems can increase the risk of conflictrelated gender-based violence.74 The main risk cited by Acheson is that the parameters programmed into the automated weapons systems could be manipulated to specifically target women or commit direct strikes on people based on their gender, such as women's rights advocates or members of the LGBTQI+ community, groups that are particularly discriminated against. While there are currently no known cases of these weapons being used to commit gender-based violence, Acheson argues that considering the prevalence of gender-based violence during conflict, these types of weapons could be wielded in unexpected ways, and a more thorough analysis of gender effects of automated weapons systems is warranted.

ASEAN countries have participated in negotiations around a treaty to ban fully automated weapons systems.⁷⁵ While South-East Asian countries are not currently leading in the production of these weapons, there is considerable risk that, absent regulations, such weapons will be adopted as part of the military arsenal in all countries.⁷⁶

3.3.2. SURVEILLANCE OF WOMEN AND WOMEN'S HUMAN RIGHTS DEFENDERS

Governments throughout the region are known to have tracked human rights defenders and other members of civil society. The rise of AI has increased the efficacy of these surveillance techniques, further endangering the safety of women's rights defenders.⁷⁷ For example, remote biometric identification through video surveillance of public areas is becoming increasingly common, notably in large cities.⁷⁸ As smart cities develop,⁷⁹ opportunities for video recording and remote biometric identification of the population will increase. In this context, women's human rights defenders are known to be included in databases, which can lead to a match if they appear in surveilled videos. A notable example includes recent reports of plans to employ facial-recognition technology to identify women defying the hijab law in Iran.⁸⁰

In addition to this, there is broad availability of AI tools that can detect trends and patterns in social media and other publicly available data, gathering intelligence on these women. Around the world, certain companies have been known to be hired by governments to track and apprehend migrants, activists, human rights defenders, political opposition and others.⁸¹

Risks also pertain to the ability to protect data, such as data used for biometric identification, and to ensure that it is not misused for surveillance or other harmful purposes. One notable example from the Asia-Pacific region includes the capture of biometric identification systems that were initially set up to aid public services and security mechanisms in Afghanistan. Since the Taliban takeover, these technologies have been claimed to have been used to detain and persecute individuals, including

⁷³ ICRC (2022). What you need to know about autonomous weapons. Available from https://www.icrc.org/en/document/what-you-need-know-about-autonomous-weapons

⁷⁴ Acheson, R. (2020). Autonomous Weapons and Patriarchy. Women's International League for Peace and Freedom with Support from the Campaign to Free Killer Robots.

⁷⁵ Non-violence international Asia (2021). Key Elements of the Treaty Banning Fully Autonomous Systems: Perspectives from Southeast Asia.

⁷⁶ Trager, R. (2022). Killer Robots are Here – and We Need to Regulate Them. Foreign Policy. Available from <u>https://foreignpolicy.com/2022/05/11/killer-robots-lethal-autonomous-we-apons-systems-ukraine-libya-regulation/</u>

⁷⁷ Root, R. (2021). Digital rights activists in Southeast Asia increasingly at risk. Devex. Available from https://www.devex.com/news/digital-rights-activists-in-southeast-asia-increasingly-at-risk-103946

⁷⁸ It should be noted that this type of biometric identification is considered high-risk in the EU Draft AI Act from April 2021.

⁷⁹ UNESCAP (2023). Smart cities in Southeast Asia: a landscape review. Available from https://www.unescap.org/kp/2023/smart-cities-south-east-asia-landscape-review

⁸⁰ Article19 (2023). "Iran: Tech-enabled 'Hijab and Chastity' law will further punish women", Available from https://www.article19.org/resources/iran-tech-enabled-hijab-and-chastity-law-will-further-punish-women/#:~:text=This%20initiative%20outlines%20various%20levels,locations%20such%20as%20the%20subway.

⁸¹ Amnesty International. (2020). Failing to do right: the urgent need for Palantir to respect Human Rights. Report. Available from https://www.amnestyusa.org/wp-content/uplo-ads/2020/09/Amnest-International-Palantir-Briefing-Report-092520_Final.pdf

women's rights activists and persons identifying as LGBTIQ+.⁸² Similar concerns have been raised across other countries in the region in line with the development of e-ID systems.⁸³ Risks pertaining to the unethical use of such data would be significantly compounded should they be linked with facialrecognition or other remote sensing technologies.



3.4 Systemic Risks: Privacy and Cybersecurity, Technosolutionism and the Digital Divide

The increased adoption of AI across a variety of sectors throughout the region also has important cybersecurity effects. AI systems both use and generate considerable amounts of data, which is not always well protected. Personally identifiable information is a kind of data that provides information about an individual, such as their location, name, image or other characteristics that would allow for their identification. This kind of data poses significant security risks for women.

Cybersecurity risks in AI are quite broad, covering all applications that could be leveraged to support WPS principles. Instances of doxxing (publishing personal information online without the person's consent) have been widely used against women in the region, notably to discredit women politicians and journalists.⁸⁴ Data breaches also put women's human rights defenders' personal and organizational safety at considerable risk, especially when they are collecting sensitive information. As reported by OHCHR, women activists in Myanmar are particularly at risk of doxxing, which is often accompanied by in-person violence or even arrests of the women.⁸⁵ Similar attacks have taken place across South-East Asia and the world.⁸⁶ Members of the LGBTIQ+ communities, who might be particularly threatened by the disclosure of personal information (especially in conservative contexts), have also been subject to online and offline harassment after data leaks.

Moreover, even without the threat of violence, many families in the region often share Internet-connected devices. Those who work outside of the home, who are more likely to be male, are more likely to leave the home with the shared device, leaving those behind without access to AI tools that might have a positive effect.⁸⁷ In this sense, when developing AI tools it is important to consider the gender digital divide, especially access to tools and device control, phenomena that can reduce the tools' reach to those who need them most.

Another adverse effect of AI in the context of WPS principles is more conceptual, but nevertheless still important. Technosolutionism is a tendency of both private-sector companies keen to sell their AI solutions in the region as well as CSOs. As one interviewee explained, "A lot of the people who are part of the collective peacebuilding community are optimistic about techno-utopian ideals." This particularly applies to the use of immature AI — AI tools or applications that are deployed in conflict and other insecure contexts without sufficiently being proven or tested, particularly with a gender-lens in mind.

⁸² Human Rights Watch (2022). "New Evidence that Biometric Data Systems Imperil Afghans", Available from https://www.hrw.org/news/2022/03/30/new-evidence-biometric-da-ta-systems-imperil-afghans

⁸³ Human Rights Watch (2021). "Myanmar: Facial Recognition System Threathens Rights". Available from <u>https://www.hrw.org/news/2021/03/12/myanmar-facial-recognition-system-threatens-rights</u>

⁸⁴ Timmerman, A (2022). Trolling, doxxing and false arrests: How governments are using tech to intimidate critics in Southeast Asia. Rest of World. Available from https://restofworld.available from https://restofworld.avail

⁸⁵ OHCHR (2023). Myanmar: Social media companies must stand up to junta's online terror campaign say UN experts. Press Release. Available from https://www.ohchr.org/en/press-releases/2023/03/myanmar-social-media-companies-must-stand-juntas-online-terror-campaign-say

⁸⁶ Venkiteswaran, G (2022). Four ways Southeast Asian journalists are under attack. The Jakarta Post. Available from https://www.thejakartapost.com/opinion/2022/05/04/four-ways-southeast-asian-journalists-are-under-digital-attack.html

⁸⁷ Tyers-Chowdury, A. and Binder G (2021). What we know about the gender digital divide for girls: A literature review. Available from https://www.unicef.org/eap/media/8311/file/What%20we%20know%20about%20the%20gender%20digital%20divide%20for%20girls:%20A%20literature%20review.pdf

The concept of technosolutionism is a particular consideration in AI for peace, where the intention of the tool is positive, but if the risks outlined above are not addressed, then the implementation might lead to adverse effects for women and women peacebuilders.



3.5. Stakeholder understanding of AI and WPS Linkages

Al and WPS issues tend to exist in separate knowledge silos. Those who have a deep technical or business understanding of AI have only superficial knowledge of the WPS agenda, and, conversely, those leading research and advocacy in WPS tend to have little knowledge of AI. This is most strikingly observed in definitions of both terms, which differ widely by sector. An exception, however, can be observed when speaking to academic researchers who have specifically studied the intersection of either AI and WPS or AI and gender.

Technical AI researchers tend to see the definition of AI from an algorithmic perspective. That is, these interviewees might discuss the type of algorithm used, such as a deep neural network or a random forests algorithm.⁸⁸ In the absence of a clear application, computational tasks would be prioritized, such as the algorithm's speed and accuracy. The interviewees might express an openness to address gender or WPS issues if they were clearly identified or outlined by someone else so that they could be approached as a set of requirements with a technical solution.

From a business perspective, AI was approached in terms of economic or commercial opportunities. Private-sector interviewees communicated enthusiasm about AI's potential to address challenges, such as environmental degradation, climate change and security. For example, one interviewee described how AI might be used in early warning systems to alert subscribers of imminent floods, how it could be coupled with Internet of Things sensors to reduce energy consumption and how it could be used in coastal surveillance to pre-empt loss of coastlines due to rising sea levels. Additionally, the interviewee discussed the use of AI in policing as an opportunity to apprehend human traffickers and protect migrants, particularly children. Private-sector interviewees had some knowledge of gender risks in AI, listing well-known examples such as discrimination in human resources algorithms. However, aside from the necessity for increased representation of women in the AI sector, they did not make a link between their work and the WPS agenda. It was clear that AI was seen as an opportunity for society more generally and that there had been little analysis of the positive and negative impacts of these applications on WPS.

CSOs interpreted AI nearly exclusively as referring to social media platforms and their algorithmic underpinnings. Their understanding of WPS was clear and largely related to the human security perspectives; they saw the WPS agenda as an issue of freedom from fear, want and need, listing these principles in the interview. While they did not clearly outline how social media platforms made use of AI, they considered the existence of the platforms to have both positive and negative effects on WPS.

Academic researchers focusing on AI and WPS were the only group that had a more elaborate understanding of the linkages between the two issues. These researchers expressed considerable concern regarding the negative effects of social media, such as polarization, gender-based violence, mis- and disinformation and facial recognition systems' contributions to a surveillance state. In this sense, academic researchers did not discuss technological biases or their potential positive effects, but rather the ways in which their use could lead to adverse societal outcomes.

Table four summarizes the differences in interviewee perspectives and definitions.

⁸⁸ Neural networks are generally understood to be a form of machine learning modelled after the human brain, using layers of interconnected nodes to compute optimal models from large datasets. Random forests is a simpler form of machine learning using groups of decision trees.

TABLE 4. APPROACHES TO AI AND WPS BASED ON INTERVIEWEE CATEGORY

INTERVIEWEE CATEGORY	AI DEFINITION	WPS DEFINITION	APPROACH TO AI AND WPS LINKAGES
Technical AI researcher	Algorithm-based	None	If clear requirements are provided for a given application, then these can be addressed
Private sector	In terms of a broad range of applications, such as environmental early warning systems and methods to apprehend human traffickers	Increasing the representation of women in AI, possibly addressing physical threats such as human trafficking	Al as an opportunity to address many social challenges, including WPS.
Civil society	Social media	The WPS agenda with a human security interpretation	Al as a threat through misogynistic content spread through social media
AI and WPS academic researchers	High-risk applications only, such as biometrics, social services, education and social media	The WPS agenda with a human security interpretation.	Al as a threat through misogynistic content spread through social media or applied to situations that could have adverse societal effects, such as surveillance



3.6. Summary of the Effects of AI Applications on the WPS Agenda

Table 5 documents two impact scales: the effects of AI application on the WPS agenda and the risks of AI application on the WPS agenda. The effect of AI application on the WPS agenda is measured on a scale of low to high, with 1 being the least favourable, 3 being neutral, and 5 being the most favourable. Four factors are considered, drawing from the four pillars of the WPS agenda: participation and representation, prevention, protection, and relief and recovery. The risk of the AI application on the WPS is measured on a similar scale, with 1 being the least risky, 3 being somewhat risky, and 5 being the riskiest.

The distinction between these two scales shows how some AI tools can have favourable effects on the WPS agenda but are risky, requiring a risk mitigation strategy, . For example, tracking tools can have a very favourable effect on WPS by allowing a more rapid response to conflict escalation and promoting women's safety. However, if improperly implemented, they can also present risks in terms of algorithmic bias, data security, surveillance and more. Table 5 provides a relevant metric for both considerations. It should be noted that Table 5 can also be used as a frame of reference when analysing and discussing the impact of an AI tool on the WPS agenda. Depending on the implementation itself, the potential effects or risk areas will vary and should be evaluated on a case-by-case basis.

TABLE 5. SUMMARY OF EFFECTS OF AI APPLICATIONS ON THE FOUR PILLARS OF THE WPS AGENDA

Potential effect on the four pillars

PR (Participation and Representation); PRE (Prevention); PRO (Protection); RR (Relief and Recovery)





D (Discrimination); S (Stereotyping); E (Exclusion); I (Insecurity);







36




There are two key considerations in efforts to ensure that AI can be leveraged to realize and comply with WPS principles. The first is mitigating the risks that AI systems present to advancing the WPS agenda, especially on social media, and other tools such as chatbots and mobile applications. The second is fostering the development of AI tools built explicitly to support gender-responsive peace in line with WPS principles.

Recent important developments in the global governance of AI include national and regional governments committing to collaborate on addressing AI risks, including minilateral initiatives at the G7, OECD and ASEAN; a UK Summit on AI Safety in November 2023; and an Executive Order in the United States that aims to address a number of the challenges discussed here, including human rights, sustainable development and cybersecurity.

The United Nations High-level Advisory Body on Al is now underway under the leadership of the Secretary-General's Envoy on Technology. Its 39 members (20 of whom are women) will develop recommendations to present to Member States at the September 2024 Summit of the Future. In this regard, the following recommendations also aim to integrate the WPS agenda into current Al governance and regulatory efforts.

1. Mainstream WPS considerations in national, regional and global dialogues on AI governance, and vice versa

While there have been significant conversations around the intersection of gender and AI, notably during the CSW67 in 2023, there is still a need for a better understanding of the security impacts of AI tools on women and gender non-conforming persons, from the grassroots to the global level. This includes ensuring that these issues are included in current policy streams on global AI governance, specifically in the text of new policies, normative documents and guidelines. While these texts almost always mention discrimination, expanding on the risks and their impacts on WPS, as detailed in this report, will be critical to ensuring that policymakers and the private sector prioritize these issues. Similarly, given the increased usage of AI systems across societies, including in peace and conflict contexts, greater attention to these issues is needed in debates on the implementation and advancement of the WPS agenda, such as in the UNSC.

There is potential to develop a framework for South-East Asian countries to consider AI from a WPS lens, particularly in light of the recently adopted ASEAN Regional Plan of Action for WPS (2022) and WPS National Action Plan development processes across the region. It is important to ensure that such efforts are inclusive during the design of such frameworks and that they stand on a foundation of multi-stakeholder dialogue. Policy-makers should also invest resources to harmonise existing frameworks on WPS, digital and cybersecurity, governance of the digital space and the tech sector.

2. Support the design of inclusive, conflict-sensitive and gender-responsive AI systems by ensuring that women have equal opportunities to lead and meaningfully participate in these processes.

There are multiple stakeholders involved in both AI regulation and WPS agenda implementation. While CSOs are increasingly working on gender and digital rights promotion, private companies and governments also have their stake, with documented tensions between rights protection and economic development. Facilitating platforms for equal engagement between civil society, governments and private sector actors – where women have equal opportunities to lead and shape the conversations – will be crucial in actioning this recommendation. Echoing the recommendations which emanated from the CSW67, proactive steps must be taken in ensuring that women and girls are part of the planning, coding and design of AI technologies.⁸⁹

3. Map and conduct gender- and human rights impact assessments of AI systems and develop policy and legislative responses including those relevant to the advancement of peace and security.

There is also a lack of clarity on what AI tools are currently being used for peacebuilding and how gender impacts could be evaluated. A catalogue of tools and methodologies for gender-impact assessments, which could be conducted before use, is also relevant. Gender and human rights impact assessments would allow stakeholders using those tools to better understand the risks involved and whether they can be mitigated. Such impact assessments should also apply to draft laws and bills prior to their adoption. This is also in line with CSW67 recommendations, which called for the adoption of "regulation on evaluation and audit requirements for the development and use of artificial intelligence to provide secure and transparent, highquality data infrastructure and systems to prevent and address human right violations and abuses, as well as gender bias". 90

4. Raise awareness and strengthen capacities of key stakeholders on risks and opportunities of AI tools for gender-responsive conflict prevention and peace efforts.

Interviews and literature reviews have shown a lack of understanding of the many links between AI and WPS. In this sense, an important outcome of this research would be to develop capacity-building and training programmes and guidelines for CSOs, the United Nations and its Member States and other stakeholders. These programmes and guidelines would facilitate better contributions to the mitigation of these risks and improved harnessing of opportunities.

5. Leverage AI for positive use such as hate-speech monitoring, fact-checking and countering disinformation on social media, accounting for the use of misogynistic and otherwise harmful gendered narratives.

Efforts to monitor hate speech and implement robust fact-checking have faltered, due in part to social media companies' struggles to effectively monitor content in South-East Asian languages. Hateful content targeting women and genderdiverse persons tends to be overlooked and under-reported. Efforts to resolve this issue by increasing localized monitoring capacities, enhancing skills on gender-responsive analysis and strengthening the accountability of social media companies remain relevant.

6. Strengthen accountability mechanisms for social media companies by enhancing users' agency in choice of providers and platforms, with specific attention to inclusive and rights-based solutions.

Alternatives to the current structure of social media platforms are increasingly being sought, notably with the development of decentralized platforms that would operate like email and allow users to use the provider of their choice. This would remove the monopoly that social media companies have on their own platform and potentially allow for increased protections across these tools. This is a commonly raised proposal by

⁸⁹ ECOSOC (2023). Commission on the Status of Women sixty-seventh session – Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls. (E/CN.6/2023/L.3).

women's digital rights organizations across South-East Asia and has been highlighted as an important step in giving Internet users more agency on the platforms they engage with. Increased transparency in the governance of these platforms, and the design of their underpinning algorithms, has also been raised as an important step forward in ensuring that the platforms are inclusive and rights-based.

BOX 6. SNAPSHOTS OF THE CHALLENGES AND OPPORTUNITIES OF AI IN THE CONTEXT OF THE WPS AGENDA FROM RESEARCH PARTICIPANTS

"AI can support highlighting the [marginalized groups'] needs and support solutions."

"But if we are not actively managing the risks, we can deepen the inequality. If we don't address [the gender inequality issue] in community policymaker standpoints, AI can perpetuate stereotypes and actively discriminate against groups that we want AI to actually support."

"Al is an opportunity to promote peace and security. But it can also harm peace and security if we don't feed them with ethical data... Al acts as it learned."

When technology is developed, "it should be tested for specific groups such as different ethnic groups, vulnerable groups and young people. Every single tool could suit every single group. All groups of people should be included in the process." Awareness of the negative effects of AI appears to centre primarily on social media's threats to women's security, notably, its capacity to incite gender-based violence, misogynistic sentiments and conflict. From a capacity-building perspective, increasing awareness of other risks and opportunities of AI tools for WPS would be relevant, notably by clearly identifying the linkages between AI and WPS, while encouraging interactions between different types of stakeholders. Additionally, there is still some work to be done on gender-impact assessments of tools used in peace and conflict contexts, notably in early warning and migration management systems to reduce uneven effects on women and minority groups.

In conclusion, AI can carry significant positive and negative effects in the context of the WPS agenda, both in South-East Asia and globally. Overall, while continued efforts to counter disinformation and misogynistic speech on social media seem relevant, opportunities to promote the positive effects of AI on WPS must be further explored to contribute to more just and peaceful societies.

ANNEX A. METHODOLOGY



Research team composition

UNU-Macau's team was led by Dr. Eleonore Fournier-Tombs and composed of several researchers, including Dr. JeongHyun Lee, Professor Preeti Rhagunath and Dr. Min Yang. All of the team members have significant experience in related domains, such as gender and Al in South-East Asia, cybersecurity and cyber resilience and Al systems. The team was advised by UNU-Macau's Director, Dr. Jingbo Huang and Dr. Jaimee Stuart, Senior Researcher at UNU-Macau.



Data collection on Gender and Al

The project used primary and secondary data sources, which were analysed together to obtain a bigger picture of AI in relation to women, peace and security in South-East Asia. Secondary data collection involved literature, reports and policy strategies related to AI and the WPS agenda. Primary data collection involved a social media analysis and stakeholder interviews across the region.

SECONDARY DATA COLLECTION

The literature review had several focuses: creating a mapping of current uses of AI for peace and conflict in South-East Asia; examining studies on known gender risks or opportunities in relation to these uses; and unearthing case studies to be further fleshed out during the social media analysis, interviews and the workshop. The review focused on academic publications and government policy documents as they relate to AI, such as national strategies, frameworks, and ethical guidance.

The secondary data collection process was undertaken by both the lead and local researchers. It included the following elements:

- > Cataloguing the uses of AI in peacebuilding, neutral (but relevant to WPS) and conflict settings for the region, according to the above framework. This involved investigating AI implementations in high-risk areas as they relate to critical technologies to understand the state of AI use in the region. This catalogue was developed through the secondary data collection process and was thereon supplemented by the interviews.
- Identifying known risks to WPS to these uses, globally. After the technologies were catalogued, a literature review was conducted on the known risks to WPS for each one.
- > Developing current AI and WPS legal framework for the region, as applicable. A mapping of laws, policies and initiatives as they relate to AI and WPS was developed across the region.

Secondary data sources

The secondary data collection process described above were derived from the following sources:

- > Academic publications.
- > Grey literature, such as UN Women or other international organization documents, government documents, policies and reports.
- > Journal or website articles from recognized sources.
- > Other journalistic investigations.



SOCIAL MEDIA ANALYSIS

Semi-structured interviews

In addition to the quantitative analysis, a series of semi-structured interviews with stakeholders and experts in the region were conducted.

18 semi-structured interviews with representatives from academia, civil society and the private sector were conducted. Interviewees came from a total of seven countries in the region. Interviewees were approached directly based on their activities and publications in this domain. The interviews lasted between 30 to 45 minutes and were transcribed and summarized for use in the analysis and reports.

The selection criteria for the interviewees involved expertise (research or practice) in either AI and gender, or peace and security and AI, or all of the above. This criterion allowed for flexibility in the likely case that interviewees only have partial expertise in the subject matter



An expert group meeting was held virtually on 4 May 2023. The meeting served as a stakeholder validation exercise and lasted for a total of two hours. The UNU-Macau team developed a meeting summary, which fed into the final research report. Expert participants who had already been identified for the interview phase were, where appropriate, invited to participate in the meeting. The UNU-Macau team offered a presentation of preliminary research results, to substantiate the discussion and validation process with the participants.



In this research, four conditions for research design were used: construct validity; internal validity; external validity; and reliability. For the purposes of this research, these were defined as follows:



The qualitative data analysis software NVivo was used to analyse this data, which allowed the research team to create a mapping of the dynamics of AI, peace, and security as they relate to gender in South-East Asia. The interviews were also coded according to a predetermined coding manual in order to obtain comparable and quantifiable outputs.

TABLE 7. RESEARCH VALIDITY

DEFINITION
To what extent do the observations measure what they are intended to measure?
To what extent does the proposed method support a cause-and- effect relationship between the treatment and outcome?
To what extent can we generalize the findings to other situations, people and countries?
To what degree do the research methods provide stable and consistent results?

Construct validity: Figure 5 illustrates the relationship between the research objectives (RO), the research questions (RQ) and the interview questions (IQ), along with other modes of data collection and analysis.

FIGURE 5. RESEARCH CONSTRUCT VALIDITY



Internal validity: From a broader perspective, the design of this research argued that gaps in understanding AI and WPS in the region result in a higher likelihood of violence, discrimination, stereotyping and socioeconomic disempowerment for women. The methodology, therefore, aimed to unearth not only new, localized WPS risks in AI, but it also sought to understand gaps in stakeholder interpretations of these issues.

External validity: There were different areas of generalization in this study. First, the research team sought to ensure that the findings from countries would inform each other. Second, the research team sought to ensure that these findings could inform policy development processes in countries beyond South-East Asia. Due to the nature of AI (a global technology) and gender (a global issue), the research team hoped that many of the findings in this study would be applicable both regionally and globally.

Reliability: In qualitative research, there is a degree of interpretability and fluidity in results that might be difficult to replicate. However, reliability was addressed in the distribution of the interview sample, which aimed to be representative of current perceptions in AI and WPS and presents different streams of thought.

In this regard, having a diverse and inclusive sample, along with the opportunity for in-depth discussion, is believed to have yielded results that would be similar to those yielded by a replication study.

Limitations of the research methodology

Not every country in the region was represented in this study. Further, given that gender impact assessments of AI tools are not regularly conducted or shared with the public and that the AI-WPS nexus is relatively new, some of the effects of AI on WPS may not be known by interviewees in the region.



All UNU-Macau research projects undergo an ethics review process through UNU's Ethics Review Board. The objective of this review is to evaluate possible risks to respondents and participants in relation to privacy, emotional or physical impact, and consent. Best practices in data collection, storage and deletion are also followed. The ethics review of this research project was completed in early December 2022.

ANNEX B. SOCIAL MEDIA ANALYSIS METHODOLOGY

Social media platforms that rely on AI technologies are widely being used for peacebuilding purposes. Peace activists and human rights defenders are using Facebook, Instagram, LinkedIn, X and others to expand their networks, create and manage content, call for action and participation and increase awareness on sustaining peace. Among all peace actors, CSOs that promote the WPS agenda stand out in terms of using social media to closely and widely engage relevant stakeholders in the peace and security agenda. Therefore, mapping out CSOs' utilization of social media can provide a bigger picture of AI technology in relation to the WPS agenda in South-East Asia.



A social media analysis was conducted to answer the research questions. The social media analysis aimed to map out the current uses of social media tools for peacebuilding purposes in Indonesia, the Philippines, Singapore and Thailand. The social media analysis was also used to find out what and how significant gendered issues and challenges were being addressed by CSOs in achieving the WPS agenda.



Methodology

Given the above context, the researchers undertook a social media analysis with a view to obtaining a bigger picture in relation to AI and WPS agenda implementation in South-East Asia. Accordingly, research questions were identified and then discussed based on the social media analysis.

Research questions included:

- > What AI technology-influenced social media tools were mainly used by CSOs in Indonesia, the Philippines, Singapore and Thailand towards implementing the WPS agenda?
- > How were social media platforms that rely on AI technology used to achieve the WPS agenda at the national, regional and global levels?
- In terms of achieving the WPS agenda in given countries, what gendered challenges/issues were mainly addressed by CSOs by using social media tools?



Primary Data Collection

The social media analysis started by accessing and collecting the qualitative and quantitative data from CSOs. After a careful review of a UN Women-provided list of CSOs, the research team identified 40 CSOs engaging in WPS-related work comprising 10 from Indonesia, 15 from the Philippines, one from Singapore and 14 from Thailand. To achieve the research purposes, the research team initially visited the identified CSOs' social media accounts. Six of the 40 CSOs did not have specific social media accounts or websites, so they were excluded from sampling, resulting in 34 validated CSOs: 10 from Indonesia, 12 from the Philippines, one from Singapore and 11 from Thailand.

The research team captured approximately 10 social media posts for each of the remaining 34 CSOs based on the following principles:

> The social media contents were directly and highly relevant to the framework of the WPS agenda.

- > The social media posts showed relatively high interactivity with their followers.
- > The captured posts covered the rich diversity of social media tools for each organization.

After removing social media posts that were irrelevant to the research objectives, the total validated sample size was comprised of 238 social media posts that met the selection criteria. These posts became the original qualitative data for the social media analysis (see Table A1).

The research team used the MAXQDA software to compile and code the sampled social media posts for analysis. All codes were categorized into three types of thematic codes: social media tools relying on Al technology; purposes; and themes (see Table A2).

TABLE A1. CODE SYSTEM FOR THE SOCIAL MEDIA ANALYSIS

TOP-LEVEL CODE	MID-LEVEL CODE
Social media tools relying on Al technology	 Facebook Faceook+Instagram live Facebook+Video/YouTube Facebook+Zoom/Online meeting tools Facebook Live Instagram Instagram+Video/Podcast/Animation X X+Facebook X+Video/YouTube Developed New Apps
Purposes	 Call for participation (refers to offline and online activities organized by CSOs, including campaigns, workshops, projects, meetings, lectures and events) Call for action (refers to audiences/public's performance change and/or actual actions to be taken) Increase awareness Advertise/disseminate information Share knowledge
Themes	 Parenting for peace Climate change/natural disaster and the WPS agenda Celebrate International Peace/Women's Day in general Peace, WPS, UNSCR 1325 knowledge in general Gender sensitivity and conflict transformation Women's empowerment Women are equally equipped with knowledge and tools Prevent/end gender-based violence Women's involvement in terrorism and radicalization Remove gendered social and cultural stereotypes and bias Increase women's meaningful participation in peacebuilding Women's security (online and offline) Defend women's human rights Women play a significant (leading) role in peace processes









The United Nations University Institute in Macau (UNU Macau) is a United Nations global think tank conducting research and training on digital technologies for sustainable development, encouraging data-driven and evidence-based actions and policies to achieve the Sustainable Development Goals.

UN University Macau

Casa Silva Mendes, Estrada do Engenheiro Trigo No.4 Macau SAR, China

www.unu.edu/macau www.twitter.com/UNUMACAU www.facebook.com/unumacau weibo.com/u/2698789630



UN Women is the UN organization dedicated to gender equality and the empowerment of women. A global champion for women and girls, UN Women was established to accelerate progress on meeting their needs worldwide. UN Women supports UN Member States as they set global standards for achieving gender equality, and works with governments and civil society to design laws, policies, programmes and services needed to ensure that the standards are effectively implemented and truly benefit women and girls worldwide. **UN Women Regional Office for Asia and the Pacific** UN Building, Rajadamnern Nok Avenue Bangkok 10200, Thailand

gps.asiapacific@unwomen.org www.asiapacific.unwomen.org www.facebook.com/unwomenasia www.twitter.com/unwomenasia www.youtube.com/unwomenasiapacific www.flickr.com/unwomenasiapacific