RESEARCH BRIEF

WOMEN, PEACE AND DIGITAL (IN)SECURITY IN SOUTH-EAST ASIA – REFLECTIONS ON DIVERSE EXPERIENCES IN THE DIGITAL SPHERE

ACKNOWLEDGEMENTS

Credits: This research report was developed by UN Women Regional Office for Asia and the Pacific. It expands on a study developed by Rebecca Emerson Keeler from Insaan Consulting Ltd., which aimed to document South-East Asian women's experiences with technology-facilitated gender-based violence. The initial study also benefited from technical contributions and review by Fitriani Bintang Timur and Gulizar Haciyakupoglu and substantive inputs from Alexandra Håkansson Schmidt and Gaelle Demolis Ebassa of the UN Women Regional Office for Asia and the Pacific.

RESEARCH BRIEF

WOMEN, PEACE AND DIGITAL (IN)SECURITY IN SOUTH-EAST ASIA – REFLECTIONS ON DIVERSE EXPERIENCES IN THE DIGITAL SPHERE

With the generous support of the Governments of the Republic of Korea and Australia.

Ministry of Gender Equality and Family

Australian Government

CYBER & CRITICAL TECH COOPERATION PROGRAM

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Digital security has emerged as a central priority for the Women, Peace and Security agenda across South-East Asian nations. In order to better understand how gender dynamics are playing out in the digital world, and specifically how these interplay with conflict and security dynamics across the region, UN Women has conducted research on the experiences of diverse women across the region.

Through forty key respondent interviews and five focus group discussions conducted in 2021 with women in the region, as well as an in-depth literature review, a number of online harms emerged as key concerns. These harms included different types of technology-facilitated gender-based violence (TFGBV), such as trolling, online hate speech and radicalization, disinformation and slander campaigns, doxxing, outing, data and privacy breaches, technology-facilitated trafficking in persons, Internet shutdowns and content access restrictions. The research found that the implications of TFGBV are particularly severe in conflict- and crisis-affected contexts due to the higher political stakes of real-life violence. Adversaries' use of TFGBV to silence women's voices and discredit their work had negative impacts on women's civic engagement and peace efforts, with some women choosing to disengage entirely from their work due to feelings of being unsafe or threatened. This not only hinders individual women's participation in public discussions, but also results in broader societal harm, as fewer women feel comfortable engaging in debate, participating in their communities or leading change, ultimately weakening the fabric of inclusive and representative societal development.

In some contexts, research indicates that in light of shrinking civic spaces and securitization of cybersecurity, these harms restrict the positive potential of information and communication technologies (ICTs) to advance gender quality and inclusive and sustainable peace. Some positive trends can also be noted: while gender considerations have historically been overlooked in cyber diplomacy forums, this is now beginning to change. There is growing recognition of gender-related cybersecurity issues in the context of international security, marking a significant shift in global discourse. To address the key issues identified in the research, this report offers the following recommendations:

Recommendation 1	Recommendation 2	Recommendation 3
Undertake holistic and evidence-based strategies to effectively prevent, counter and respond to incidences of TFGBV, particularly in politically volatile and conflict- and crisis-impacted contexts.	Advance knowledge, capacities and tools that ensure that women and persons with diverse sexual orientation, gender identity and expression and sex characteristics can safely and equitably lead the development and governance of ICTs and digital platforms, including advancing online civic engagement and digital peacebuilding.	Ensure that cyber- and digital security laws, policies and strategies are gender-responsive, informed by principles underlying the Women, Peace and Security agenda, and adherent to international law and human rights obligations.

1.

INTRODUCTION

Technological advancements made throughout the last decades have been lauded for setting off a fourth industrial revolution by fundamentally changing the way in which we live, work and socialize.[1] Further, these advancements have largely reshaped the dynamics of the global security landscape. However, social media has increasingly become a platform for disinformation, hateful narratives and violent extremist groups to gain support for their agendas. This, in combination with rampant misogyny and xenophobia, is actively contributing to the rise in social tensions, polarization and inflammation of public debate across societies.

Dovetailing with these shifts, cybersecurity has emerged as a priority agenda for dialogues on international and national security. The protection of critical infrastructure and safeguarding of public assets are increasingly integral to national security strategies. In addition, initiatives to foster multilateral cooperation on cybersecurity matters are accelerating. However, while the links between international and national security and cyber-related insecurities are widely recognized, there is still little scrutiny of the community-level impacts of harms and attacks in digital spaces, how these are experienced differently across genders, or the human security perspectives that have been largely overlooked in said dialogues.

Women and persons with diverse sexual orientation, gender identity and expression and sex characteristics (SOGIESC) are differently and disproportionately affected by online harms.[2] Women public figures, including politicians, journalists and human rights defenders, are further exposed to these risks to a larger extent than everyday Internet users as a direct result of their work and civic engagement. There are numerous reports of women and gender equality advocates being pushed to disengage from their work because of the technology-facilitated harms they have faced. This is effectively pushing women out of leadership and decision-making spaces and risks fuelling the persistent backslide of gender equality gains.

Notwithstanding these risks and harms, there has been a notable shift in the use of technologies and innovation to foster sustainable development. Information and communications technologies (ICTs) are increasingly being used as integral tools in peace efforts to facilitate mediation, peace dialogues, consultations and early warning systems. As technological developments advance — particularly in the realm of peace and security — it is crucial to ensure that gender considerations are thoroughly embedded in these processes. While the research field is still nascent, feminist academia is starting to explore how the Women, Peace and Security (WPS) agenda could provide a guiding framework.

1 Schwab, K. (2016). *The Fourth Industrial Revolution: what it means, how to respond*. World Economic Forum. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

2 Global Network of Women Peacebuilders (GNWP) and ICT4Peace (2021). *Women, Peace, and Security and Human Rights in the Digital Age: Opportunities and Risks to Advance Women's Meaningful Participation and Protect Their Rights*. https://gnwp.org/wp-content/uploads/PolicyBriefGNWP-2021c.pdf

Digital security has yet to be explicitly referenced in any of the United Nations Security Council Resolutions that constitute the WPS agenda. However, digital security issues are increasingly being discussed as part of localization processes across South-East Asian nations. Although the policy spaces linking cybersecurity and the WPS agenda are evolving, evidence on gender dynamics in cyberspace remains sparse and scattered. Responding to the dearth of information on the topic, this report seeks to better understand the digital security landscape in South-East Asia as experienced by women activists, human rights defenders, public figures and Internet users at large. The insights and recommendations gleaned from the underlying research will better inform programming and regional and global policy- and decision-making related to the digital landscape.[3] [4]

BOX 1. TERMINOLOGY

Many terms and concepts are used to describe risks and security measures on digital platforms, often lacking standardized definitions. The terms 'digital security' and 'cybersecurity' are often used interchangeably, although there are nuanced differences between the two. For the purpose of this research, the following definitions are used:

- **Cybersecurity** refers to a "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices and technologies that can be used to protect the cyber environment and organization and user's assets," including technical infrastructure, applications, services and telecommunications systems.[3]
- **Digital security** is a broader term that refers to "the economic and social aspects of cybersecurity, as opposed to purely technical aspects and those related to criminal law enforcement or national and international security."[4]

This report seeks to understand digital security implications and their gendered dynamics; however, it also explores key cybersecurity concerns voiced by women in South-East Asia, recognizing their interconnected nature.

3 International Telecommunications Union (2008). Series X: Data networks, open system communications and security – Telecommunication security: Overview of cybersecurity, Rec. ITU-T X.1205 (04/2008).

4 OECD (2022). OECD Policy Framework on Digital Security, OECD Publishing, Paris, https://doi.org/10.1787/a69df866-en

BOX 2. METHODOLOGY

This report offers a summary of key findings from research and data collected by UN Women and Insaan Consulting Ltd in 2021. The initial data collection focused on user experiences in South-East Asia through a gender lens with a focus on four areas: (i) Internet access and user profiles; (ii) cyber-harms; (iii) recourse to justice; and (iv) opportunities and challenges for positive online engagement for peace and social cohesion. Insaan Consulting collected data from May to October 2021 via interviews and focus group discussions, focusing on 10 South-East Asian countries.[5]

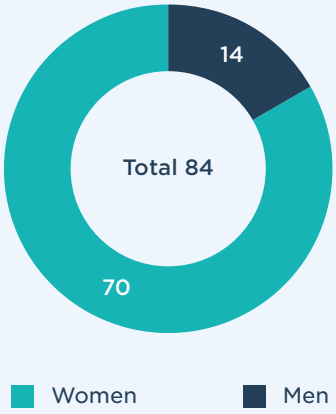
Data collection was hampered and delayed due to COVID-19 restrictions. Although the data collected from respondents and focus group discussions (FDGs) remain relevant to the research, since then, findings from primary data collection have been supplemented by more recent literature review of relevant research reports, statistics and relevant media coverage of issues relating to gender and digital security, as well as analyses and documentation of debates relating to the WPS agenda.

Building on this data, this report aims to deepen the understanding of:

- Diverse experiences of online harms and digital security threats in South-East Asia;
- How gendered online harms affect civic engagement and peace efforts led by women and gender equality advocates; and
- The implications this has for implementing the WPS agenda in South-East Asia and beyond.

For more information on the methodology and methodological limitations, see Annex A.

RESEARCH PARTICIPANTS



Moreover, four respondents identified as having diverse SOGIESC and two respondents identified as living with one or multiple disabilities.

40

Key informant interviews were conducted with women politicians, activists, human rights defenders, CSO representatives and academics from South-East Asia.

5

Focus group discussions, engaging a total of 44 persons, were held with CSO representatives and individuals with diverse SOGIESC in Indonesia and the Philippines.

1

Validation workshop was held with 19 national and regional CSOs from South-East Asia from 3 to 5 June 2022.

5 Brunei, Cambodia, Indonesia, Lao People's Democratic Republic, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Viet Nam. Note that at the time of data collection, Timor-Leste had not been recognized as an ASEAN member state, and was therefore not included in the initial research scope.

2.

WOMEN, PEACE AND SECURITY IN THE DIGITAL WORLD

The Women, Peace and Security agenda was first established in 2000 through the adoption of UNSCR 1325. This was the first Security Council Resolution that linked gender equality and international peace and security, recognizing that women and men are differently impacted by conflict and that women face the brunt of many conflict-related harms. UNSCR 1325 was the result of decades of strong advocacy by grassroots women's movements and civil society, echoing their calls for the necessity of women filling central roles in conflict prevention and resolution processes and in building sustainable peace. UNSCR 1325 also recognizes that it is imperative to ensure that women's perspectives and experiences are reflected in the solutions and responses that are put forward to address security challenges.

An additional nine WPS-related resolutions have followed UNSCR 1325, broadening global perspectives on the roles that women fill in peace processes and the ways in which they are differently impacted by conflict and other forms of insecurity. Each new resolution has expanded the WPS agenda to account for new intricacies and emerging security issues.

The global community is increasingly recognizing that social and gender inequalities have magnified the human security implications of cyberspace, where organized misogyny campaigns and violent narratives against women have taken root. This devolution necessitates a new set of skills and protection measures for women, particularly those who are involved in any form of peace effort.

For the last five years, the UN Secretary General's Annual Reports on WPS have recognized the implications of technologies and cyberspace to the agenda; the scope of these issues has been continuously expanding. The reports from 2019 and 2020 primarily focused on online violence and the importance of bridging the gender digital divide.[6] Since then, the focus has grown to encompass several other factors that are affecting women's safety and well-being. For example, the 2021 report recognized digital technologies' potential to leverage peace efforts and facilitate inclusive mediation processes. It also warned of the increasing impacts of digital surveillance on women and women's rights defenders.[7] The 2022 report went further to recognize cyberspace as a possible domain for conflict and raised concerns regarding the new challenges that increasingly autonomous weapon systems pose, systems that are rarely developed with sufficient — or any — gender analysis.[8] Lastly, the 2023 report emphasized that "online and offline violence and gender-based hate speech continue to undermine women's participation" and that women's meaningful participation in negotiating peace is significantly obstructed by the weaponization of digital technologies.[9]

6 S/2019/800; S/2020/946
7 S/2021/827
8 S/2022/740
9 S/2023/725

In 2023, the 67th Commission on the Status of Women also made references to the importance of the digital sphere to the WPS principles. The Commission recognized "the contribution of digitalization to the full, equal and meaningful participation and involvement of women in peace processes, conflict prevention, conflict resolution and peacebuilding."[10]

Cybersecurity and the use of emerging technologies in the context of peace and security have been outlined as key priority areas under the UN Secretary General's policy brief, 'A New Agenda for Peace'.[11] The brief outlines that digital tools have created unforeseen avenues for far-reaching civic engagement, particularly for youth. However, the same tools have simultaneously been used to restrict civic participation by limiting access to audiences or information or by tracking, surveilling or otherwise harassing those who make their voices heard (particularly in protest), with women politicians and human rights defenders being among those most heavily targeted. In recognition of these issues, the brief's priority action 11 calls for the prevention of the weaponization of emerging domains while promoting responsible innovation.

Lastly, it is important to recognize that debates on international security and cybersecurity have taken place in a number of multilateral forums. These should not be considered siloed; these processes must be harmonized in order to effectively build strategies and well-founded policies around digital security and WPS. To better substantiate such discussions, the remainder of this chapter will offer an overview of broader UN debates on digital security and cybersecurity as well as localized efforts to conceptualize these issues within the WPS agenda.

2.1. Gender and cyber diplomacy

While the linkages between peace, security and the digital world are increasingly in the global limelight, the recognition of the importance of these issues is far from recent. Much of the multilateral work on this has been advanced by the Groups of Government Experts (GGE) on the use of ICTs in the context of international security. In total, there have been six GGEs working on the topic since 2004.[12] To broaden the debate to all UN Member States, in 2018, the General Assembly established an Open-Ended Working Group (OEWG) on ICTs in the context of international security. Effective from 2019 to 2020, a new five-year OEWG on the topic has been established.

Even though online threats and harms are experienced differently across genders, women have been underrepresented in policy and decision-making forums relating to technology and digital security, including in cyber diplomacy forums. Historically, **men have outnumbered women 2 to 1 in multilateral forums on ICTs in the context of international security**, such as the GGEs. Women's representation in these dialogues has, however, seen an increase since 2019.[13]

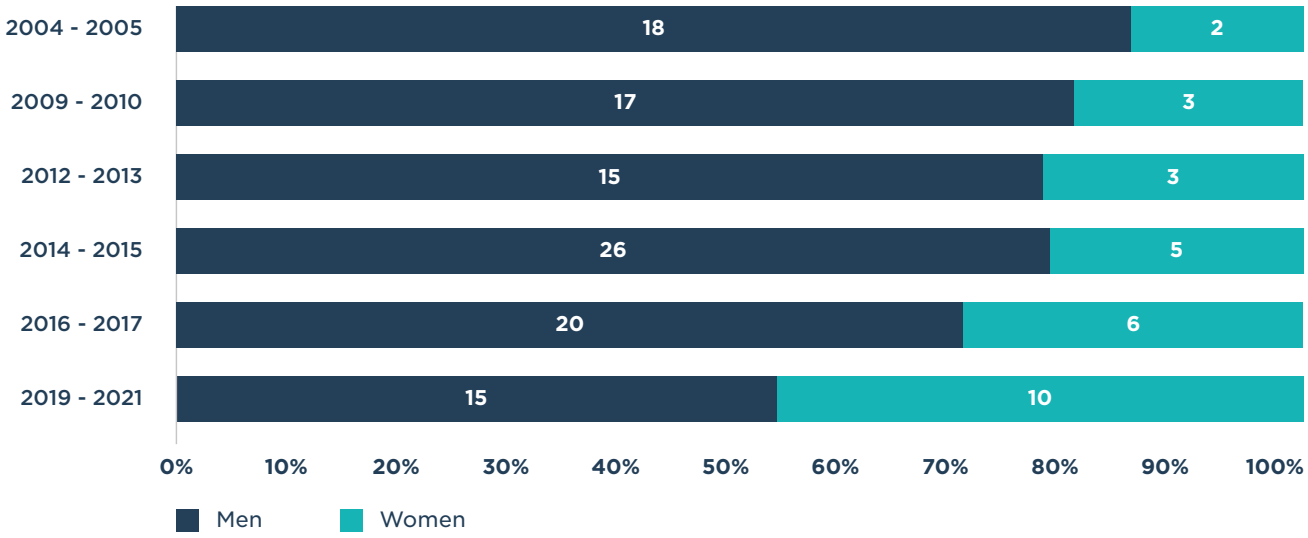
10 67th Commission on the Status of Women (2023). Agreed conclusions: Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls. https://documents.un.org/doc/undoc/ltd/n23/081/71/pdf/n2308171.pdf?token=WbbTqdZtvNx352T4d6&fe=true

11 United Nations (2023). *Our Common Agenda Policy Brief 9: A New Agenda for Peace.*

12 1st GGE (2004-2005); 2nd GGE (2009-2010); 3rd GGE (2012-2013); 4th GGE (2015-2015); 5th GGE (2016-2017); 6th GGE (2019-2021). During these periods, the following Asian nations have been members of the GGEs: China, India, Indonesia, Japan, Malaysia, Pakistan, Republic of Korea and Singapore.

13 United Nations Institute for Disarmament and Research (2019). *Factsheet – Gender in Cyber Diplomacy.* https://unidir.org/publication/fact-sheet-gender-in-cyber-diplomacy/

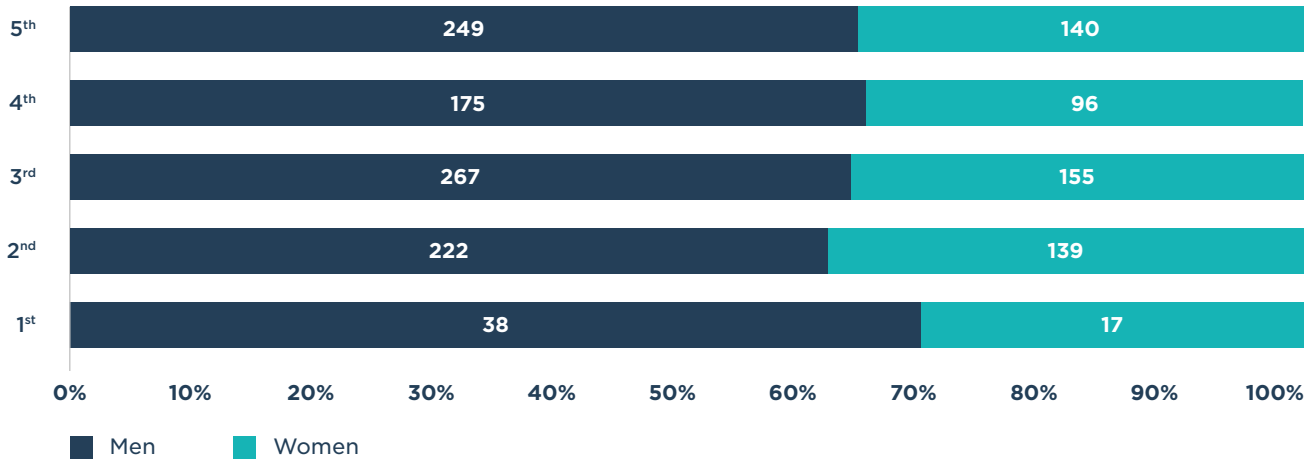
FIGURE 1. GENDER BALANCE IN CGEs ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY



Source: United Nations Institute for Disarmament and Research (2019). Factsheet – Gender in Cyber Diplomacy[15]

Similar gender disparities have been observed across the OEWGs. Out of the 414 participants in the first OEWG (2019-2020), 32 per cent were women and 68 per cent were men. Representation in leadership positions was even more unequal; only 24 per cent of the delegations were led by women.[15] Thus far, women's representation in the dialogues has been slightly higher in the second OEWG (2021-2025), averaging 37 per cent compared to men's 63 per cent.

FIGURE 2. GENDER BALANCE IN THE SUBSTANTIVE SESSIONS OF THE 2ND OEWG FOR ICTS IN INTERNATIONAL SECURITY (2021-2025) - As of December 2023



Source: UN Women, based on provisional lists of participants for the OEWG for ICTs in international security (2021-2025)[17]

14 Ibid.
15 Ibid.
16 A/AC.292/2021/INF/1/Add.1; A/AC.292/2022/INF/1; A/AC.292/2022/INF/3; A/AC.292/2023/INF/2; A/AC.292/2023/INF/4. Note that while the 6th substantive session of the 2nd OEWG had been held at the writing of this report, the provisional list of participants was not available at the time of data collection.

Cyber diplomacy forums have historically overlooked gender considerations. However, this trend is slowly changing; gender-related cybersecurity considerations in the context of international security are gaining recognition. Several delegations to the OEWG have raised the need to mainstream gender in cyber norm development and implementation (for more information, see Box 2). The importance of developing tailored capacity-building efforts has also been raised, along with calls for strengthening women's leadership in cybersecurity governance. Lastly, it has been stressed that these efforts need to be underpinned by a better understanding of the gendered dimensions of cybersecurity.[17] Nevertheless, there is still progress to be made in terms of translating these calls into tangible actions and ensuring that gender issues are systematically included in the agenda.

BOX 3. UN FRAMEWORK FOR RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE

Although UN Member States have agreed that international law should apply to cyberspace, there is still little consensus as to how. The GGEs and OEWGs have played important roles in advancing the foundation for a global cybersecurity governance framework. Their efforts have led to the formulation of a UN Framework for Responsible State Behaviour in Cyberspace. The Framework consists of four components:

1) Recognition of the applicability of international law to cyberspace;
2) Eleven voluntary and non-binding norms for responsible state behaviour in cyberspace;
3) Confidence-building measures to strengthen resilience against cyber harms; and
4) Cyber capacity-building to harness the benefits and mitigate the risks of increased connectivity.[19]

The Framework has given significant attention to the 11 norms, which outline what states can and cannot do in cyberspace, including eight encouraged and three discouraged actions.

ASEAN member states have played an active role in developing these norms; it was the first regional body to subscribe to them in principle. Currently, Malaysia and Singapore are co-chairing the working committee for the development of a long-term implementation roadmap for the norms across ASEAN Member States.[20] This outlines a key opportunity for ASEAN Member States to explore localized strategies for mainstreaming cybersecurity into WPS approaches and for designing conflict-sensitive and gender-responsive cybersecurity frameworks.

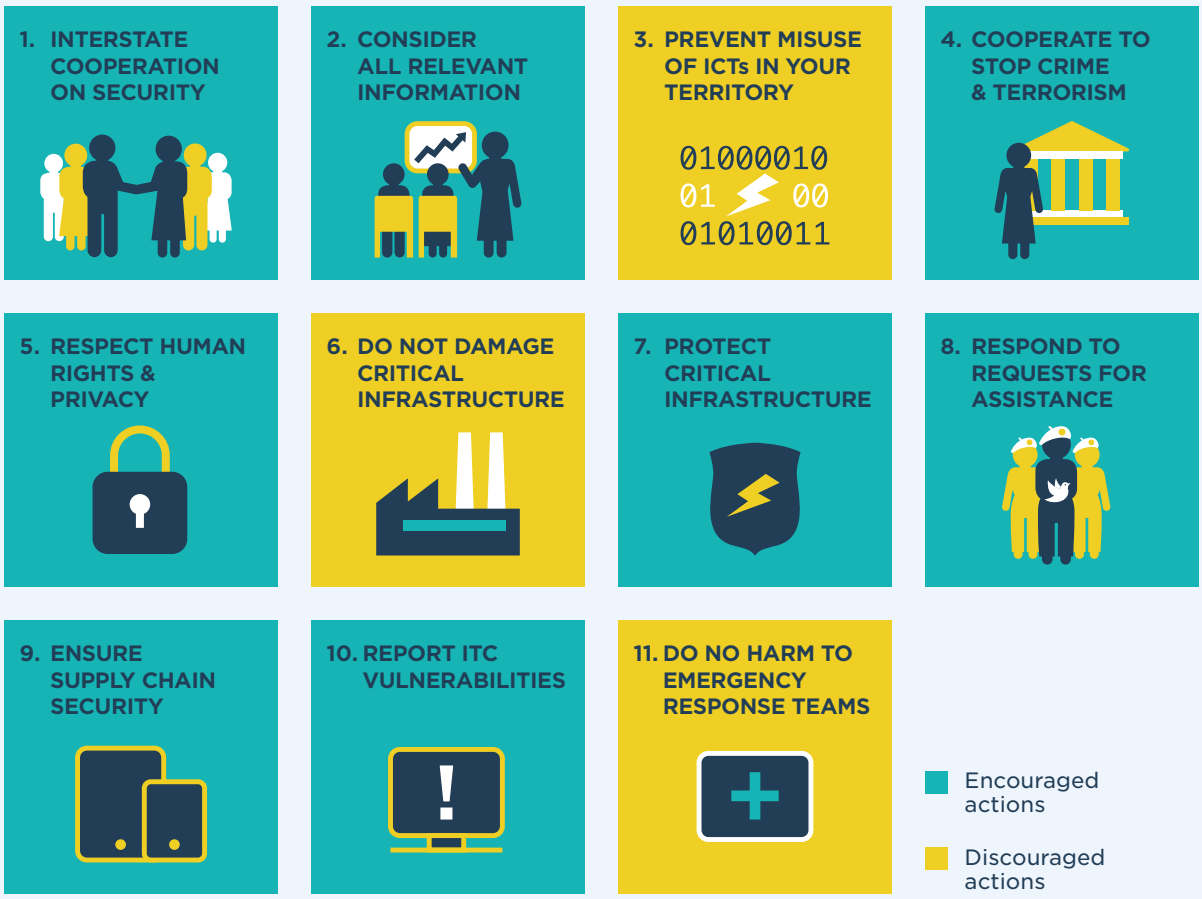
However, while the 11 norms and the UN framework at large offer a consensus-based framework for diplomatic relationships in cyberspace, it is not cognizant of the gender dynamics in play. As states adopt and operationalize the norms, it is important that they do so in conjunction with gender equality frameworks and other related policies, such as regional, national and local WPS commitments.

17 United Nations Institute for Disarmament and Research (2021). *Advancing Gender Considerations in the Cyber OEWG*. https://unidir.org/advancing-gender-considerations-in-the-cyber-oewg/

18 Australian Strategic Policy Institute (2022). *The UN norms of responsible state behaviour in cyberspace: Guidance on implementation for Member States of ASEAN*. https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf

19 ASEAN Cybersecurity Cooperation Strategy (2021-2025). https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

UN NORMS OF RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE



ASEAN MEMBER STATES' PARTICIPATION IN OEWG/GEE 2004-2021

Malaysia

UN GGE ★★
UN OEWG ★

Indonesia

UN GGE ★★★
UN OEWG ★

Philippines

UN GGE ★★
UN OEWG ★

Brunei

UN GGE
UN OEWG ★

Thailand

UN GGE
UN OEWG ★

Singapore

UN GGE ★
UN OEWG ★

Vietnam

UN GGE
UN OEWG

Cambodia

UN GGE
UN OEWG ★

Myanmar

UN GGE
UN OEWG

Lao P.D.R.

UN GGE
UN OEWG ★

★ Each time OEWG/GEE the respective country has participated in

Note: This analysis is based on research conducted by the Australian Strategic Policy Institute.

2.2. UNSC debates on cybersecurity and emerging technologies

Over the last decade, the Security Council has held numerous informal meetings to address cybersecurity in the context of international security, hybrid warfare, conflict prevention, attacks on critical infrastructure, digital education, capacity building and countering hate speech. In the past, gender considerations have, at best, been recognized at the fringe of these conversations. Recently, however, awareness of the importance of these issues has increased; in the last few years, an increasing number of Member States have raised gender inequality issues in their UNSC interventions. An overview of relevant UNSC meetings can be found in Annex 2.

For instance, during the 2021 Arria-formula meeting[20] on 'Delivering accountability through innovation and partnership: Harnessing technology to deliver justice for war crimes, crimes against humanity and genocide', the Estonian delegation stressed the importance of addressing the specific needs of survivors of sexual and gender-based violence.[21] Moreover, a number of Member States, including Australia, Costa Rica and Switzerland, highlighted the disproportionate impacts of online harms on women and LGBTIQ+ communities and referenced the relevance of the WPS agenda in addressing these harms in statements delivered during the 2023 Arria-formula meeting on 'The responsibility and responsiveness of states to cyber-attacks and critical infrastructure'.[22]

On 29 June 2021, the first-ever UNSC open debate on cybersecurity was held to discuss ways to maintain international peace and security in cyberspace. While gender concerns were not outlined in the main discussion points of the meeting, some related issues surfaced. Izumi Nakamitsu, the UN High Representative for Disarmament Affairs at the time, stressed the need to support women's participation in digital decision-making, and the Irish delegation stressed that more efforts are needed to "overcome the gender digital divide and to expand the participation of civil society, technical experts, academics and the private sector" in decision-making processes.[23]

Dialogues relating to ICTs in the context of international peace and security have been focusing on the implications of emerging technologies, such as artificial intelligence. On 18 July 2023, the UNSC held its first-ever open debate on artificial intelligence, addressing the opportunities and ramifications of deploying these technologies in conflict- and post-conflict settings. Although gender was not an integral feature in these discussions, it emerged as a key discussion point in a subsequent Arria-formula meeting held on 19 December 2023, where Council Members were urged to consider how artificial intelligence could be used to support the implementation of the WPS agenda, and the full, equal and meaningful participation of women, including in conflict and post-conflict situations.[24] This was among the first occasions where the WPS agenda was explicitly referenced in these debates

20 Arria-formula meetings are informal meetings convened at the initiative of a member or members of the United Nations Security Council. Due to their informal character, Arria-formula meetings usually have no record and no outcomes.

21 Permanent Mission of Estonia to the UN (2021). *Statement by DPR Gert Auväärt at UN Security Council Arria-formula meeting on Delivering Accountability through Innovation and Partnership*. https://un.mfa.ee/statement-by-dpr-gert-auvaart-at-un-security-council-arria-formula-meeting-on-delivering-accountability-through-innovation-and-partnership/

22 United Nations Security Council (2023). *Letter dated 6 June 2023 from the Permanent Representative of Albania to the United Nations addressed to the President of the Security Council.* S/2023/412

23 United Nations Security Council (2021). *Press Release: 'Explosive' Growth of Digital Technologies Creating New Potential of Conflict, Disarmament Chief Tells Security Council in First-Ever Debate on Cyberthreats*. https://press.un.org/en/2021/sc14563.doc.htm

24 Permanent Mission of the United Arab Emirates to the United Nations New York, Permanent Mission of the Republic of Albania to the United Nations New York (2023). Concept Note: "Arria-formula" meeting of the UN Security Council Members. Artificial Intelligence: Its impact on hate speech, disinformation and misinformation. https://teamup.com/4777015/attachment/01HHQD2SYDV3MB95JD8YEAMD56/Concept%20note%20Arria%20on%20AI_hatespeech-mis-disinformation%20-%20%2813%20Dec%202023%29.pdf?hash=42043ea7c643ce12ce8426e346b2a2ae70fe89ea74804def2c073b3b33b9a770

2.3. Local approaches to digital security and the WPS agenda in South-East Asia

As global policy debates on digital security and the WPS agenda advance, rapid progress is being made at the national and regional levels worldwide. Although digital security has yet to be referenced in any of the UNSCRs that make up the WPS agenda, at least 19 (17 per cent) out of 109 National Action Plans (NAP) on WPS that have been adopted around the world reference issues relating to digital security, cybersecurity, cybercrime or the disproportionate effects of online harms on women.[25]

Cybersecurity is an emerging priority for the Association for South-East Asian Nations (ASEAN) and its member states at large. The issue was identified as central to regional security concerns in the ASEAN Regional Study on WPS.[26] It has subsequently been outlined as a key priority in the 'ASEAN Regional Plan of Action for WPS' (RPA-WPS), adopted on 16 November 2022. The ASEAN RPA-WPS includes four specific priority actions that are related to cybersecurity: committing to integrate sexual and gender-based violence programming to prevent cybercrimes; preventing cybersecurity threats and other emerging threats to peace and security at large; supporting gender mainstreaming efforts across the national security sector, including when it comes to cybersecurity; and identifying legal and policy reforms and capacity building activities that can "prevent violence within online spaces, counter the spread of misogynist views online and prevent cybercrimes and online bullying and harassment, especially toward women, children and others who may be especially targeted."[27]

The Philippines, after the adoption of its 4th NAP-WPS (2023 – 2033), became the first country in South-East Asia to recognize cybersecurity considerations as part of its WPS commitments. The NAP-WPS recognizes the importance of cybersecurity to the country's emerging security landscape and includes specific action points on ensuring women's meaningful representation, participation and leadership in cybersecurity planning, design, governance and law enforcement efforts, including strengthening the capacities of women's grassroots organizations, peacebuilders and human rights defenders on cybersecurity and digital peacebuilding.[28] Cybersecurity is also mentioned in the '2023-2028 Regional Action Plan on WPS of the Bangsamoro Autonomous Region of Muslim Mindanao' (BARMM) in the Philippines, which outlines the importance of gender-responsive, conflict-sensitive and peace-promoting regional policies and frameworks to advance cybersecurity and the need to support further research and evidence generation initiatives on emerging WPS issues, such as cybersecurity.[29]

25 Internal review of WPS-NAPs, with English translation available, valid throughout 2024. The NAPs have been scanned for the keywords cyber, digital, online and Internet. NAPs who only reference online and digital communication as a means of raising public awareness on WPS, without recognizing the impact of online harms on women and girls, have not been categorized as referencing digital security-related issues. References to said issues were found across the following countries' NAPs: Denmark (2020-2024); Estonia (2020-2025); Ireland (2019-2024); Italy (2020-2024); Kenya (2020-2024); Malawi (2021-2025); Namibia (2019-2024); Netherlands (2021-2025); Norway (2023-2030); Philippines (2023-2033); South Africa (2020-2025); Sri Lanka (2023-2027); Timor-Leste (2024); Ukraine (2020-2025); United Arab Emirates (2021-2024); United Kingdom (2023-2027); Ukraine (2020-2025); United States (2023); Viet Nam (2024-2030).

26 ASEAN Secretariat, USAID, UN Women (2021). *ASEAN Regional Study on Women, Peace and Security.* https://asean.org/book/asean-regional-study-on-women-peace-and-security/

27 ASEAN Regional Plan of Action for Women, Peace and Security. https://asean.org/asean-regional-plan-of-action-on-women-peace-and-security/

28 Philippine National Action Plan on Women, Peace and Security (2023-2033). https://peace.gov.ph/national-action-plan-women-peace-security/?fbclid=IwAR05tWevOlE6j8qC7x-v93gMr5Opc_I-VH85BlMsVmP75iOZtGQvcfn1LuRA

29 BARMM RAP-WPS (2023-2028

Countries such as Viet Nam and Timor-Leste have since followed suit. On 25 January 2024, Viet Nam adopted their first-ever NAP-WPS. It recognizes cybersecurity as an emerging security issue under the WPS agenda and outlines the need for support to women to respond to cyber threats, incidents and other challenges.[30] In January 2024, Timor-Leste adopted its second NAP-WPS. Similarly, this NAP-WPS recognizes the need to better understand security threats in cyberspace, such as gender-based attacks, cyber-enabled trafficking in persons and the spread of gendered misinformation.[31]

These advancements are important because they have effectively placed digital- and cybersecurity on the WPS agenda across South-East Asia. However, as echoed by most of the NAPs referenced above, there is a need to generate evidence and develop further thinking on how these commitments can be implemented as part of broader WPS strategies in the region. To accelerate this momentum and to inform further efforts, the next chapter of this report addresses key digital security concerns experienced by women in South-East Asia, as viewed from a WPS lens.

30 Viet Nam NAP-WPS (2024-2030).
31 Timor-Leste NAP-WPS (2024-2028). https://asiapacific.unwomen.org/en/digital-library/publications/2024/02/nap-unsc-1325-2024-2028

3.

DIVERSE EXPERIENCES OF DIGITAL (IN)SECURITY IN SOUTH-EAST ASIA

With the rapid rate of digitization, online spaces have become new frontiers for conflict and violence, with conflict actors increasingly relying on ICTs to recruit members and garner support for their agendas, spread propaganda and violent narratives, and to finance and facilitate their operations. Prevailing gender norms influence many of these tactics, which tend to amplify existing inequalities. Digital platforms are also increasingly used to facilitate gender-based violence, trafficking in women and other forms of exploitation, particularly in conflict-affected areas.[32]

Women living in contexts with entrenched gender inequalities tend to experience online violence at higher rates. Recent reports indicate that 88 per cent of women in the Asia-Pacific region have been exposed to online violence.[33] Globally, these harms have included instances of gender-focused misinformation and slander campaigns (in 67 per cent of total recoded cases of online violence); hacking and stalking (63 per cent of the cases); hate speech (65 per cent of the cases); and threats of physical harm (52 per cent of the cases).[34] These percentages may underestimate the prevalence; the number of unrecorded cases is expectedly high, as research suggests that only 25 per cent of women report harmful online behaviour to the social media platforms on which it occurs.[35]

While women at large face disproportionate risks of being exposed to online harms, women public figures (including politicians, journalists, human rights defenders and peacebuilders) face an added layer of risk, as they tend to be systematically targeted because of their work and civic engagement. In research examining online interactions from 2020 to 2021, women's human rights defenders (WHRDs) were deemed to be the second most frequently targeted group of human rights defenders across Asia.[36] Out of 145 identified cases of attacks against WHRDs' freedom of expression during this period, close to 40 per cent occurred online, including cases of data breaches and incitements to violence, misogynistic and sexist insults and other derogatory remarks that were often accompanied by death and rape threats.[37] WHRDs are central to gender-responsive peace efforts; obstructions to their work substantially hinder the advancement of the WPS agenda.

To better understand how these dynamics play out in South-East Asia, UN Women and Insaan Consulting Ltd. Interviewed 84 persons (70 women and 14 men, out of which four identified as having

32 The Asia Foundation (2020). *Violent Conflict, Tech Companies and Social Media in Southeast Asia: Key Dynamics and Responses.* https://asiafoundation.org/publication/violent-conflict-tech-companies-and-social-media-in-southeast-asia/
33 The Economist Intelligence Unit (2020). *Measuring the prevalence of online violence against women.* https://onlineviolencewomen.eiu.com
34 *Ibid*
35 *Ibid*
36 FORUM-ASIA, *Defending in Numbers* (2021). https://www.forum-asia.org/uploads/wp/2021/06/Defending-in-Numbers-A-Message-of-Strength-from-the-Ground-for-web.pdf
37 *Ibid*

diverse SOGIESC) from South-East Asia to better understand, from a gender lens, which key challenges they face on digital platforms. Key outcomes from these interviews have informed the contents of this chapter; quotes from respondents are included to illustrate South-East Asian women's experiences of online harms. The quotes, including the country of origin of the respondents, have been anonymized in the interest of study participants' safety.

3.1. Understanding technology-facilitated gender-based violence through a WPS lens

While online harms are not new, there is little consensus on a common definition and terminology that encompasses these acts. To date, this has resulted in difficulties in producing comparable data and knowledge on the topic. To address this challenge, UN Women has advocated for the development of a common and comprehensive definition to fully capture the range of harms that women and gender-nonconforming individuals face on digital platforms — **Technology-facilitated gender-based violence (TFGBV)**.

TFGBV constitutes "any act that is committed or amplified using digital tools or technologies causing physical, sexual, psychological, social, political or economic harm to women and girls because of their gender."[38] It encompasses a number of harms, such as misogynistic hate speech, online threats of offline violence, doxxing, trolling, image abuse, the sharing of deep-fake content, and any other efforts that aim to silence and discredit women online.[39]

While TFGBV touches upon violence against women at large, it has specific implications in conflict and post-conflict contexts. First, online harassment is closely linked with offline violence. Digital spaces tend to reflect the typically higher levels of violence observed in conflict- and post-conflict contexts. With a lower threshold for violent acts and the normalization of violent narratives in public debate, online harms and harassment are more likely to spill over to in-person attacks. Acts such as online stalking or the non-consensual attainment of personal data can further enable or facilitate real-life violence, harassment and killing, particularly in precarious, conflict or otherwise volatile environments.

> *"I was worried someone was stalking me online... [This] is a conflict area with conflicts between Muslims and Christians. We could be followed, raped or killed then thrown off a cliff.*
>
> – Women's Rights Organization Representative, South-East Asia

Second, the political stakes in conflict-affected areas are high. These contexts tend to be prone to mis- and disinformation. Social media allows for the rapid spread of misleading information in conflict contexts, particularly where social media acts as a main news source.[40] Adversaries targeting women's rights and gender equality advocates often falsely accused them of representing extremist or immoral ideals, effectively undermining their advocacy in the eyes of the public.

> *"One colleague is attacked regularly for human rights activism online by male information operations. They create fake Facebook IDs and are paid to spend the day attacking activists. She is a Muslim woman (minority group) and the [...] operations team says she is spreading extremism to 'brainwash people'. They use personal details to attack people and it hurts.*
>
> – Women's Human Rights Defender, South-East Asia

38 UN Women (2024). Placing gender equality at the heart of the global digital compact: Taking forward the recommendations of the sixty-seventh session of the commission on the status of women. https://www.unwomen.org/sites/default/files/2024-03/placing-gender-equality-at-the-heart-of-the-global-digital-compact-en.pdf, p. 8.

39 UN Women. FAQs: Trolling, stalking, doxing and other forms of violence against women in the digital age. https://www.unwomen.org/en/what-we-do/ending-violence-against-women/faqs/tech-facilitated-gender-based-violence

40 Stavros, A., Phalen, S., Almakki, S., Nacionales-Tafoya, M. and Garcia, R. A. (2023). *Disinformation in Conflict Environments in Asia*. Gerald R. Ford School of Public policy, University of Michigan. https://diplomacy.umich.edu/sites/wdc/files/2023-05/disinformation-in-conflict-environments-in-asia.pdf

In consultations with UN Women, women from South-East Asia reported that online attacks previously tended to be one-offs or targeted certain high-profile individuals, they are becoming increasingly systematic in the way they target certain issue-based movements and actors, such as feminist organizations. This has serious implications for women's ability to participate in social and political processes and may constitute a hindrance to their enjoying their fundamental human rights.

The following online harms, identified during interviews and focus group discussions, are of specific concern for women Internet users across South-East Asia. These will be addressed in further depth throughout this chapter.

TABLE 1. EXAMPLES OF AI APPLICATIONS IN A WPS CONTEXT

Cyber-facilitated trafficking in persons	The use of digital platforms to move persons across borders for sexual or labour exploitation, including to facilitate recruitment, exploitation and exertion of control and pressure over victims.[42]
Data breaches	Any event that exposes confidential, sensitive or protected information.
Disinformation	False information that intentionally misleads, such as propaganda intended to influence elections or foster conflict.
Doxing	Private or identifying information distributed about a person on the Internet with deliberate negative intent.
Hate speech	Any type of communication, whether in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor.[43]
Internet shutdowns	Intentional disruption of the Internet or electronic communications, rendering them inaccessible or effectively unusable for a specific population or within a location, often to exert control over the flow of information.[44]
Outing	Involuntary public revelation of another's sexual orientation and gender identity, which can be done offline or online.
Radicalization	The act of causing someone to adopt radical positions on political or social issues.
Trolling	Deliberately provoking or upsetting individuals or groups online by posting inflammatory, irrelevant, or controversial messages.

41 Group of Experts on Action Against Trafficking in Human Beings (2022). *Online and technology-facilitated trafficking in human beings: Summary and recommendations*. https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-summary-/16804a5e10c

42 UN Strategy and Plan of Action on Hate Speech (2019). https://www.un.org/en/genocideprevention/documents/advising-and-mobilizing/Action_plan_on_hate_speech_EN.pdf

43 Access Now. *Internet Shutdowns and Elections Handbook*. https://www.accessnow.org/guide/Internet-shutdowns-and-elections-handbook/

3.1.2. CYBER-ENABLED TRAFFICKING IN WOMEN

Conflict increases the risks of trafficking, including sexual trafficking, and other forms of exploitation. The WPS agenda recognizes trafficking in women as a critical security concern that is exacerbated in conflict and crisis settings; trafficking women in these contexts may be considered a form of conflict-related sexual violence. In addition, crisis and political instability exacerbate trafficking risk factors such as economic hardship and displacement.[44]

Hence, even countries without an ongoing armed conflict that face other forms of insecurities, crises or humanitarian needs also face a heightened risk of trafficking, both through traditional and digital channels.[45] Women and girls are particularly vulnerable to these crimes because they are more likely to experience the push and pull factors of trafficking, such as lacking decent work and personal identification documents, and because they tend to underestimate online risks and harms.[46]

> *"They read an advertisement on social media that offered a job at the fashion store in Yogyakarta city. They provided a good salary (US$275) to the victims and picked them up from home taking them to Yogyakarta. When they arrived at Yogyakarta, the company prostituted them via an online platform instead of employing them as promised.*
>
> – Civil Society Representative, South-East Asia

With increased Internet usage, online platforms are increasingly becoming home to criminal activities. The use of social media and other online platforms to recruit and lure persons into precarious labour situations increased in South-East Asia during the COVID-19 pandemic, as strict lockdown measures and mobility restrictions pushed more people to seek alternate ways of earning a decent living. Respondents expressed strong concern regarding these trends, highlighting that this, coupled with a low level of awareness of risks or inability to judge the authenticity of job ads and offers, resulted in women and girls being trafficked for the purpose of sexual exploitation. Respondents stressed that awareness-raising and digital literacy initiatives are important components in holistic responses to these issues.

> *"These Facebook groups operate like shipping logistics firms. They recruit on Facebook with fraudulent job opportunities, engage families to pay large amounts for travel (the families believe the more they pay the safer the girl) only for their daughters to end up in sex work, forced labour of simply disappear at the hands of the traffickers or in transit countries.*
>
> – Representative of an anti-trafficking organization, South-East Asia

3.1.3. DATA AND PRIVACY BREACHES

Hacking and data breaches are increasingly posing threats to politicians, journalists, human rights defenders and activists and everyday Internet users. Data breaches are often coupled with other online harms, such as doxing, and can also lead to in-person violence and persecution, depending on the nature of the leaked data.

> *"If the photos are leaked, they are the ones being blamed instead of the person who leaked the photos. So, essentially, we are getting degraded and judged, instead of the people who violated other people's data privacy.*
>
> – Women's Student Group Representative, South-East Asia

The risks of data breaches and hacking have grown along with the increased use of online platforms. Many users have insufficient knowledge of online data and privacy protection practices. Some informants highlighted the importance of improving education and awareness in these areas. Respondents from several South-East Asia countries highlighted the risks of phishing,[47] fraud, hijacking[48] and extortion as pressing information security

44 Bigio, J. and Vogelstein, R. (2019). *Understanding Human Trafficking in Conflict*. Council on Foreign Relations. https://www.jstor.org/stable/resrep21427.4
45 Ibid.
46 Yoshi Torigoe, *How Technology Can Combat Human Trafficking* (2019). https://news.itu.int/how-technology-can-combat-human-trafficking/
47 Phishing involves an individual being contacted by email, telephone or text message by someone posing as a legitimate institution to trick the individual into providing sensitive data; https://www.merriam-webster.com/dictionary/phishing
48 Cyber hijacking is a cybercrime which involves a hacker seizing control of software, network communications or computer systems. This can be used to gain access to, or steal, data or private information. https://worldtechjournal.com/what-is-cyber-hijacking-types-cyber-hijacking/

risks. Student informants in the Philippines said that ransomware[49] had been used to encrypt their files; they were subsequently extorted for personal and professional content in order to regain access to their files. The students explained that women targets of data breaches often face a losing battle, where the wider community tends to resort to victim blaming rather than focusing on the means of holding perpetrators accountable.

Deploying specialized tools (e.g. spyware[50]) to attain personal data is increasingly — and systematically — being used to target human rights defenders, journalists and political opposition. The Pegasus spyware has raised particular concerns because it can access messages, calls, the microphone and biometric data in devices without the user downloading or clicking malicious files or links. Between 2016 and 2018, the Pegasus spyware was used to target an estimated 50,000 individuals (including in at least two South-East Asian countries),[51] many of whom are activists or high-profile individuals.[52] Human rights defenders have warned that the deployment and use of Pegasus spyware and similar surveillance software poses a threat to women in particular because it amplifies the risk of harassment, fear and self-censorship, harms that already disproportionately affect women.[53]

3.1.4. DISINFORMATION AND SLANDER CAMPAIGNS

Conflict and post-conflict contexts offer particularly fertile breeding grounds for disinformation to spread.[54] Malicious actors are growing increasingly adept at utilizing social media and other online platforms to target audiences with disinformation. Disinformation activities adversely affect social cohesion, often target women and other vulnerable groups and can be weaponized to disrupt the efforts of peacebuilders and rights activists.

The gender dimensions of disinformation remain underexplored.[55] Recognizing this vacuum, experts and practitioners are drawing attention to 'gendered disinformation'[56] and to myriad examples where disinformation involved gendered narratives or had acute gendered implications. For example, there have been numerous accounts of women in public office being exposed to politically motivated slander campaigns or misogynistic harassment.

This emerged as a prominent theme in the interviews for this study; respondents recounted reports of women political candidates being framed in ways that could criminalize their behaviour or result in falsely altering their campaigns. Respondents from the Philippines in particular brought up the case of a prominent woman politician and her experiences of being the target of disinformation campaigns and fake news, particularly during election periods. The false claims were often of a sexual nature, accusing the politician of "scandalous" behaviour. The attacks also extended to her daughters, who became targets of non-consensual, sexually explicit, deep-fake videos.[57]

Online disinformation is also commonly recognized to have exacerbated hate speech and atrocities committed against the Rohingya communities in Myanmar, leading to rampant killings, mass rapes and other forms of sexual- and gender-based violence.[58] Gendered narratives and disinformation have also been used to fuel anti-Muslim sentiments

49 Malicious software designed to block the user's access to digital data or devices until a sum of money is paid or other action is taken.
50 Malicious, covert software designed to obtain information about a target's computer activities.
51 Marczak, B., Scott-Railton, J., McKune, S., Razzak, B. A. and Deibert, R. (2018). Hide and seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/
52 Amnesty International (2022). *How Amnesty Tech Uncovered the Spyware Scandal: The Pegasus Project*. https://www.amnesty.org/en/latest/news/2022/03/the-pegasus-project-how-amnesty-tech-uncovered-the-spyware-scandal-new-video/
53 Rina Chandran and Maya Gebeily (2021), *Analysis - From Middle East to India, Women 'violated' in Pegasus Hack*. https://www.reuters.com/article/tech-women-surveillance-idUSL8N2P91KX
54 Anwar Mhajne, *et al., A Call for Feminist Analysis in Cybersecurity: Highlighting the Relevance of the Women, Peace and Security Agenda* (2021). http://eprints.lse.ac.uk/112410/
55 UK Government, *Quick-Read Guide: Gender and Countering Disinformation* (2020). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866353/Quick_Read-Gender_and_countering_disinformation.pdf
56 For various interpretations of the term, see "Gender-based disinformation: advancing our understanding and response," 20 October 2021, https://www.disinfo.eu/publications/gender-based-disinformation-advancing-our-understanding-and-response/
57 Martin Petty, *Harassed but unbowed, Philippines VP to take on 'poisoned chalice' role* (2019), https://www.reuters.com/article/us-philippines-drugs-opposition-idUSKBN1XH12U, Pola Rubio, *Robredo biggest fake news victim: fact-check group* (2022). https://www.tsek.ph/robredo-biggest-fake-news-victim-fact-check-group/ and Raymund Antonio, "Tricia Robredo follows sister in seeking NBI help over fake video scandal", *Manila Bulletin* (2022). https://mb.com.ph/2022/04/26/tricia-robredo-follows-sister-in-seeking-nbi-help-over-fake-video-scandal/
58 UN Human Rights Council, Report of Independent International Fact-Finding Mission on Myanmar (2018). https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_64.pdf

across Myanmar at large, often including narratives where Muslim men are portrayed as violent sexual predators who seek to convert or sexually abuse women from the Buddhist majority population.[59]

3.1.5. DOXING

Doxing is the act of publishing private or identifying information about a person online without the person's consent, often with malicious intent. The published information may include a target's home or work address, phone number or even personal information about their family members or friends. Often, this information is fragmented among different sources, but malicious actors deduce the information from otherwise innocuous-seeming facts (e.g. combining a school mascot with geographic information and other clues to deduce a home town).

> *"In 2012, [a notable international woman activist] came to [our country] to discuss feminism with us. [An extremist group] used social media to tell people where the event was located and they violently attacked us. A similar incident happened again in 2016 with thugs widely using social media to mobilize a violent rally.*
>
> – Women's Human Rights Defender, South-East Asia

Doxing can have serious security implications that can translate into real-life harms, such as stalking and physical attacks. This is of particular concern in conflict-affected or otherwise volatile political contexts, where human rights activism, civic engagement and certain peacebuilding activities may be perceived as contentious, and where people engaged in these activities may risk arbitrary arrest, persecution, physical attacks or even killing as a result of their work.

Respondents shared a number of cases where WHRDs across South-East Asia were the targets of doxing attacks and feared physical attacks as a result. One respondent also recounted an incident in which extremist groups shared the personal information of a notable international woman activist visiting the country. After their event location was leaked, both the activist and members of the group hosting her suffered from attacks. In another country, informants raised the issue of a woman politician suffering personal attacks after having her phone number and address publicly disclosed during a televised court hearing. Within hours, she had received almost 2,000 text messages and phone calls containing threats and derogatory comments.[60]

3.1.6. HATE SPEECH AND RADICALIZATION

Hate speech includes expressions that advocate, incite, promote or justify hatred, violence or discrimination against a person or group of persons for a variety of reasons, such as because of their gender, sexual orientation, ethnicity or religion. Online misogyny and hate speech targeting women rapidly increased during the COVID-19 pandemic. According to a data analysis conducted by UN Women, UNFPA and Quilt.AI, misogynistic language significantly in the Asia-Pacific region increased between October 2019 and October 2020, with misogynistic statements increasing by a staggering 22,384 per cent in Thailand, 953 per cent in the Philippines and 140 per cent in Singapore. Other countries saw a more modest yet unacceptable increase (e.g. 21 per cent in Indonesia), and Malaysia even saw a 19 per cent decrease.[61]

It is important to consider that hate speech tends to fuel conflict factors, as these often draw from historical social tensions and inequalities. In some contexts, these narratives are politicized to maintain entrenched power structures.[62] Respondents stressed that incidences of hate speech in South-East Asia notably targeted people with diverse SOGIESC and women who are sympathetic to, or working on, gender equality.

59 Schmeltzer, A., Oswald, T., Vandergriff, M. and Cheatham, K. (2021). *Violence Against the Rohingyia: A Gendered Perspective*. PRAXIS: The Fletcher Journal of Human Security, Tufts University. https://sites.tufts.edu/praxis/2021/02/11/violence-against-the-rohingya-a-gendered-perspective/

60 See also Maila Ager, "De Lima condemns disclosure of her cell-phone number, home address," *Philippines Inquirer* (2016). https://newsinfo.inquirer.net/817393/de-lima-condemns-disclosure-of-her-cell-phone-number-home-address

61 UN Women, UNFPA and Quilt.AI (2021). COVID-19 and Violence Against Women: The Evidence Behind the Talk – Insights from Big Data Analysis in Asian Countries. https://data.unwomen.org/publications/covid-19-and-violence-against-women-evidence-behind-talk

62 Liebowitz, J., Macdonald, G., Shivaram, V. and Vignaraja, S. (2021). *The Digitalization of Hate Pseech in South and Southeast Asia: Conflict-Mitigation Approaches*. Georgetown Journal of International Affairs. https://gjia.georgetown.edu/2021/05/05/the-digitalization-of-hate-speech-in-south-and-southeast-asia-conflict-mitigation-approaches/

Moreover, hate speech coupled with disinformation has the potential to amplify resentment towards certain groups and individuals, thereby driving radicalization and the spread of extremist ideologies on social media.[63] These narratives often contain gendered statements to ensure that the messaging is compelling to a broader audience.[64] Respondents in some of the targeted countries were particularly concerned about increases in extremist-backed hate speech and the tendency for such groups to use intermediaries, including public figures, to amplify gender-harmful messages.

> *"Online dating sites are filled full of extremist men who try to shift women's adherence to sharia to fundamentalism saying they should use the burqa, saying women deserve this as punishment from God. Others suggest women should stay at home. If you put in certain search terms into google, such as 'Muslim', 'dating' or 'online', very often women see this content from Wahabi inspired men. [A local] newspaper included in their front page a flier for advertising child marriage. On- and offline harms amplify one another.*
>
> – Representative from a Women's Organization, South-East Asia

3.1.7. INTERNET SHUTDOWNS AND CONTENT ACCESS RESTRICTIONS

States across the world are increasingly deploying Internet shutdowns and other types of access restrictions, often legitimizing them under the light of maintaining public order and national security, quelling protests or reducing the spread of disinformation during election periods.[65] International bodies such as the Human Rights Council have sounded alarms at the increased use of Internet restrictions during critical moments, such as elections, peaceful protests and other democratic movements, as well as in times of conflict and other crises.[66]

Like the rest of the world, Asia has also experienced internet shutdowns.[67] The implications of Internet shutdowns are felt strongly in conflict settings, as they hinder civil society's and peacebuilders' operations and outreach.[68] Shutdowns also make it more difficult for the broader public to access and verify information, which can have adverse and escalatory effects during conflicts and unrest.[69] The UN High Commissioner for Human Rights has also recognized that Internet shutdowns "undermine access for women and girls to critical support and protection, exacerbating the gender divide."[70]

Respondents also explained certain types of websites and website content had been blocked, including information on gender and women's rights, which was particularly concerning given the need for accurate information on these topics. It was also stressed that Internet shutdowns have real-life security implications because users can no longer access information on ongoing armed confrontations or access information on the availability of necessary basic services. It also prevents people from accessing essential services and exercising their digital and human rights.

> *"In 2016, my friend and I established a project with a website and Facebook page to promote non-violent, peaceful activism and protest the cybersecurity bill. During that time, our website and Facebook page received lots of trouble. The government inserted blocked features so not many people could find it.*
>
> – Women's Human Rights Defender, South-East Asia

63 Centre for Strategic and International Studies, *The Current State of Terrorism in Indonesia: Vulnerable Groups, Networks, and Responses* (2018). https://www.csis.or.id/uploaded_file/publications/the_current_state_of_terrorism_in_indonesia_-_vulnerable_groups__networks__and_responses.pdf

64 UN Women (2019). Who's behind the keyboard? A gender analysis of terrorism and violent extremism in the online space in Bangladesh, Indonesia, Malaysia and the Philippines. https://asiapacific.unwomen.org/en/digital-library/publications/2019/03/whos-behind-the-keyboard

65 EngageMedia (2022). *What is an Internet shutdown? A Guide for South and Southeast Asia civil society.* https://engagemedia.org/2022/Internet-shutdowns-south-southeast-asia/

66 United Nations Human Rights Council (2019). *Rights to freedom of peaceful assembly and association – Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*, A/HRC/41/41.

67 Freedom House (2023). *Freedom on the Net 2023 – The Repressive Power of Artificial Intelligence.* https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf

68 UN Women, *Empowered Women, Peaceful Communities* (2020). https://asiapacific.unwomen.org/sites/default/files/Field%20Office%20ESEAsia/Docs/Publications/2019/08/ap-pve-UNW19290_BROCHURE_002_WEB-compressed.pdf

69 OHCHR, *Internet Shutdowns and Human Rights*, (2021). https://www.ohchr.org/sites/default/files/Documents/Press/Internet-shutdowns-and-human-rights.pdf

70 United Nations Human Rights Council (2022). *Internet Shutdowns: Trends, Causes, Legal Implications and Impacts on a Range of Human Rights*, A/HRC/50/55.

3.1.8. OUTING

Closely linked to doxing, respondents engaged in LGBTIQ+ rights activism raised how 'outing' posed a significant challenge to their work. Outing refers to the involuntary public revelation of another's sexual identity, which can be done online or offline.[71] LGBTIQ+ activist respondents shared how members of the community have been outed for reasons ranging from revenge when relationships ended to cases of business competition. Outing often incurs several personal risks for the outed individual, particularly in contexts where gender non-conformity or same-sex relationships are criminalized or where LGBTIQ+ communities are heavily scrutinized.

Respondents highlighted that exposing their gender identity and/or sexual orientation to hostile actors or to conservative family members sometimes resulted in exclusion or self-imposed community exile, where the target had to disengage from their activism and sometimes even relocate. Some respondents stated that transgender people were deemed most at risk from outing, with devastating impacts not only on their livelihoods, but also on their freedom of movement and safety. Focus group participants also shared an example of police officers doxing and then outing individuals with diverse SOGIESC by publicly re-posting photos and screenshots from online groups and social media posts — an example of outing that resulted in attacks from the wider community.

3.1.9. TROLLING

Trolling occurs when someone deliberately tries to upset others online, which can result in a 'pile-on' in which others join the attack.[72] Trolls usually spread inflammatory content to provoke emotional responses or to disrupt public discussions. The attacks can either be carried out by individuals or in coordinated and sometimes well-financed operations.

> *"Me and my young female staff were harassed by government trolls on Facebook. They spread fake news about me and another organization, saying that we were being paid by the government [thereby undermining our legitimacy as independent human rights organizations].*
>
> – Human Rights Organization Representative, South-East Asia

Respondents reported that trolling has posed significant challenges to their work. Across the region, respondents reported being distressed by male Internet users who trolled feminists by appropriating and sometimes sexualizing emancipatory feminist quotes or by producing anti-feminist memes.[73] In some countries, respondents noted that trolls have launched campaigns to brand LGBTIQ+ rights activists as sex workers while sharing sexually explicit photos of them, which fuelled a backlash against LGBTIQ+ communities.

Trolling of women holding positions such as journalists, activists and peacebuilders, face a higher risk of being targeted by trolling than others. Trolling of women holding such positions is growing increasingly common, particularly among right-wing movements; it has been recognized as a widespread tactic to discredit women and the causes they work for.[74]

> *"A woman who worked for an NGO posted on her social media site during the last elections that the president was lazy and she was attacked online and threatened by trolls saying they would pour acid on her. Her case is still ongoing and she has now left the country.*
>
> – Human Rights Defender, South-East Asia

71 Gary Hicks and Hillary Warren (2009). "Whose Benefit? Gay and Lesbian Journalists Discuss Outing, the Individual, and the Community," *Journal of Mass Media Ethics*. https://doi.org/10.1207/s15327728jmme1301_2

72 Trolling", Australian Government, eSafety Commissioner, https://www.esafety.gov.au/young-people/trolling

73 Visual content, typically with an attempt at humour and often replicated and spread rapidly by Internet users. Not all memes are attempts at trolling.

74 Di Meco, L. (2023). *Monetizing Misogyny: Gendered Disinformation and the Undermining of Women's Rights and Demcoracy Globally*. https://she-persisted.org/wp-content/uploads/2023/02/ShePersisted_MonetizingMisogyny.pdf

UNESCO has highlighted a prominent example from South-East Asia in the case of Maria Ressa[75], who, after publishing an investigative report in 2016, received more than 90 online misogynistic and racist messages within one hour[76] and has since been targeted by a number of coordinated trolling campaigns. About 60 per cent of the online attacks that were directed against her included attempts to undermine her professional credibility; over 40 per cent of the attacks targeted her on personal grounds (out of which 34 per cent were classified as misogynistic, sexist or sexually explicit).[77]

3.2. Digital Insecurity Implications for Gender-Responsive Peace Efforts

Although the list of harms addressed insofar is far from exhaustive, the preceding sections have shed light on the many and diverse harms that women face online, focusing on the types of harms identified as most pressing by women in South-East Asia. While the tactics and expressions of these harms differ, respondents stressed how they all result in heavy mental burdens and often physical risks for women and actors working to promote gender equality and women's rights. This is taking such a vast toll on the women's rights community that many of its members are choosing to disengage from their work entirely.

> *"If I think too much about the things that have happened to me online, I will not be able to continue feminist activism. It is too emotionally draining.*
>
> – Women's Human Rights Defender, South-East Asia

This was echoed during the research validation workshop that UN Women held from 1 to 3 June 2022, where women's rights advocates stressed that online attacks hamper their work and contributions to peace efforts. Workshop participants also explained that their families and friends were sometimes targeted due to their affiliation with the rights advocate. The lack of sufficient support mechanisms further exacerbates these issues, leaving women and gender non-conforming persons who have been exposed to online harms less resilient to the systemic attacks they encounter.

Women peacebuilders and WHRDs are also increasingly sounding the alarm regarding state actors perpetrating online surveillance and judicial harassment, in which state actors may have been responsible for some online harms.[78] On a broader scale, this restricts online freedom of expression, assembly and peaceful process, which poses a serious roadblock to women's enjoyment of their digital- and human rights.[79]

The muffling effect of online attacks on women's voices also keeps them from reaping the benefits of technological advancements, including those that aim to strengthen peace and security efforts. ICTs are increasingly used to facilitate peace processes, for example, by enabling public online platforms for peace consultations that feed into official peace talks, monitoring ceasefires, and coordination among negotiating parties.

75 2021 Nobel Peace Prize Laureate and a prominent journalist from the Philippines.
76 Nermine Aboulex, *The Chilling: Global Trends in Online Violence against Women Journalists* (UNESCO, 2021). https://unesdoc.unesco.org/ark:/48223/pf0000377223
77 Posetti, J., Maynard, D. and Bontcheva, K. (2021). *Maria Ressa: Fighting an Onslaught of Online Violence – A Big Data Analysis*, International Center for Journalists. https://www.icfj.org/sites/default/files/2021-03/Maria%20Ressa-%20Fighting%20an%20Onslaught%20of%20Online%20Violence_0.pdf
78 *Ibid*
79 See A/HRC/41/41.

> *"My team often received sexist comments and backlash when we socialized historical concepts of LGBTQI+. We decided to postpone this topic and instead bring it to an offline format. People in the digital sphere do not filter their thoughts, unlike when we conduct an offline meeting.*
>
> – Woman public figure, South-East Asia

Given the increased spread and accessibility of ICTs, many actors have stressed the potential for technological solutions to make peace processes more inclusive of historically marginalized groups, such as women.[80] This may prove to be a vast missed opportunity if adequate protection mechanisms are not put in place to ensure that women can safely engage with these tools and meaningfully participate in their design.

Lastly, while social media has opened new venues for women's civic engagement, it has also enabled women to be more engaged as conflict actors. Whereas women have generally been engaged as combatants in conflict to a far lower extent than men, some reports are indicating that women are increasingly using their "online presence and networks to contribute to tactical support, propaganda and partisan attacks."[81] In South-East Asia, this has primarily been observed in the tactics of some violent extremist groups and has also been observed in some trafficking networks.[82] While this specific conclusion did not emerge in the primary data collection that was undertaken for the purpose of this report, it may be a consideration that requires attention in further research efforts.

80 Buzatu, A.., Santos, A. F., Lakehal, D.n Pourmalek P. and Zelenanska, M. (2021). *Women, Peace and Security and Human Rights in the Digital Age: Opportunities and risks to advance women's meaningful participation and rights*, Global Network of Women Peacebuilders and ICT4Peace Foundation. https://gnwp.org/wp-content/uploads/Policy-BriefGNWP-2021c.pdf

81 The Asia Foundation (2020). *Violent Conflict, Tech Companies and Social Media in Southeast Asia: Key Dynamics and Responses*. https://asiafoundation.org/wp-content/uploads/2020/10/Violent-Conflict-Tech-Companies-and-Social-Media-in-Southeast-Asia.pdf, p. 27

82 *Ibid*

4.

OBSTACLES TO GENDER-RESPONSIVE DIGITAL SECURITY IN SOUTH-EAST ASIA

This report has addressed a number of interpersonal harms faced by women Internet users in South-East Asia and described how they are used to damper the gender- and women's rights movement across the region. Respondents also recounted systemic obstacles that they faced in terms of conducting their work through digital channels. This chapter offers an overview of these challenges, which more closely relate to governance issues and the broader policy space relating to cyberspace.

4.1. Narrowing of civic and operational spaces

Many of the harms raised by the respondents in this report are closely interlinked with broader trends of shrinking civic space across the region, where women and gender rights advocates in particular face specific challenges. There have been numerous accounts of well-funded and coordinated attacks against high-profile female targets; state-sponsored actors have been accused of being behind some of these campaigns.

Global Internet freedoms have also been on a steady decline throughout the last decade. Free expression online is increasingly coming under attack, with persons facing judicial harassment, legal repercussions, physical attacks and even killings for their statements on digital platforms.

> *"Women and girls are most vulnerable. We are sexualized as soon as we speak. They use this as a weapon against the female activists who speak up in general. [...] I have to keep my profile low. I am being watched off[- and] online. I prefer to meet in person and use private messaging.*
>
> – Women's rights activist, South-East Asia

Online smear campaigns targeting activists, and unionists have been documented across the region, including the use of online trolls to shape narratives.[83]

These trends, including the surge in anti-feminist and anti-gender sentiments across the region, are closely related to the rise of conservative and polarized politics. A number of WHRDs from the broader Asia-Pacific region have voiced concerns that far-right movements are coopting human rights spaces at the national, regional and international levels, which is hampering their human rights activism.[84] A number of participants in the June 2022 research validation workshop echoed concerns regarding the growing strength of anti-gender movements.

83 Solidar (2022). *Erosion of Civic Space in Asia: A Regional Overview.* https://solidar.ch/wp-content/uploads/2022/02/Solidar-Asia-2021-v5.pdf

84 International Women's Rights Action Watch (IWRAW) Asia Pacific (2023). *Universalising Gender Equality Norms: CEDAW's Critical Role in Protecting Women's SoGIESC rights.* https://www.iwraw-ap.org/wp-content/uploads/2023/02/Universalising-Gender-Equality-Norms-CEDAWs-critical-role-in-protecting-womens-SOGIESC-rights.pdf

As support for women's rights and gender equality is on the decline, so is funding and resources dedicated to women's civil society organizations. Respondents noted that they are currently facing a "resource crunch," with limited human capital, funding and time to fully operate. While some respondents believed that stronger online engagement could facilitate resource mobilization by expanding and diversifying their audiences and support networks and could offer a workaround to the increasingly challenging operational spaces they were facing, many online harms have effectively pushed women offline, reducing the organizations' outreach and fundraising opportunities.

The lack of access to affordable cybersecurity solutions and opportunities to strengthen digital capacities exacerbate the online harms that target women. Given already scarce resources, few women's organizations can afford to hire cybersecurity experts or license software to protect their devices and data.

4.2. Weak accountability mechanisms on digital platforms and for big tech

Most online threats unfold in or are facilitated through social media platforms, the majority of which are owned by large technology companies. Although the platforms have community guidelines and policies, respondents explained that their responses to online harms and TFGBV remain insufficient. Focus group participants criticized digital companies for prioritizing work on issues concerning fraud and e-commerce rather than on policies to create a safe space for women, with reports of TFGBV being deprioritized or unaddressed.

At the validation workshop, some CSO representatives raised concerns about digital platforms' failure to address discrimination and harassment of minorities on their platforms. A lack of safe digital spaces has led to women missing out on opportunities offered by digital companies and being unable to exercise their digital and human rights.

> *"[One of the largest social media companies in the region] has many public policy staff in the region, but when there are issues they refer to HQ and we never hear anything more. They say 'we consulted CSOs', but we have not seen positive change.*
>
> – Digital Rights Defender, South-East Asia

There are also concerns regarding the inaccessibility and ineffectiveness of social media reporting mechanisms for online harms, harassment and harmful content. Respondents explained that some women politicians reported fake accounts registered under their names to a large social media platform. However, they recounted having to utilize their personal contacts within the company to have the accounts removed. Other respondents, who did not have access to such contacts, had vastly different experiences; their cases were not resolved. In Myanmar, respondents discussed how harmful social media posts in Burmese were not addressed because not enough employees at the company could read either the Burmese or Rohingya language or understand local cultural nuances in the messaging. An informant from a social media company suggested that its approach was to empower users to independently take action to report.

Lastly, respondents working for digital rights groups noted that responding to TFGBV requires civil society to cooperate with social media and digital rights organizations because they often have direct referral paths to and from government institutions. However, some informants also outlined significant obstacles when discussing their engagement and interactions with social media companies. Activists mentioned attending events hosted by digital companies (with examples shared by respondents in Indonesia and Thailand), but when cases were taken to the companies, the companies played a limited role in addressing the concerns raised. The companies' eagerness to engage varied; study participants recounted that some companies did not respond to cases raised by activists, especially when issues related to state or transnational disinformation. Similar issues were raised at the UN Women validation workshop; participants called for

social media companies to consult with CSOs in initial dialogues and decision-making leading up to and throughout system and procedure development.

4.3. Securitization of cybersecurity and related legislation

Cybersecurity is a highly securitized topic, where the protection of the cyber realm is primarily seen as a national security priority. These sentiments have also been echoed across UN debates on the topic. For example, in the first-ever UNSC debate on cybersecurity in the context of international security in 2021, a large part of the discussions were focused on cyberspace as a growing venue for conflict between state and non-state actors both within and across national borders.[85] While an important aspect to consider, this perspective is currently dominating the cybersecurity debate at the expense of overlooking the human- and community-level impacts that online harms can have. Cybersecurity initiatives, therefore, tend to focus on deterrence, national defences and mitigating attacks on critical infrastructure and less on the effects on users or the increasingly prominent roles that digital platforms play in shaping the social fabric.[86]

Nevertheless, a slight shift in these narratives can be observed at the international, regional and national levels. Some government institutions are investing attention in the gender dimensions of some areas of their cybersecurity and protection policies. For instance, in the Philippines, the Philippine Commission on Women and the Philippine National Police have acknowledged digital violence against human rights defenders and civil society.[87] The Safe Spaces Act (RA no. 11313), which the Philippines adopted in 2018, includes a dedicated article (Article II) that penalizes online, gender-based sexual harassment.[88]

The research shows that some cybersecurity laws and criminal codes have facilitated the prosecution of women activists and human rights defenders.[89,90] Privacy and cybersecurity legislation appeared to have been used more for criminalizing criticism of the government than for providing protections for ICT infrastructure and users. Moreover, some privacy and cybersecurity legislation reviewed do not provide sufficient protection for ICT infrastructures and users. Legal experts are increasingly calling for human rights principles to be taken into account when formulating national cyber regulations, including the right to privacy, freedom of expression, digital access, data privacy and security. [91]

Respondents suggested that establishing response and recourse mechanisms that go beyond traditional law enforcement is paramount because the re-stigmatization linked to the criminal space drives under-reporting in survivors and causes secondary harms in the form of mental, emotional and physical tolls. Focus group participants from LGBTIQ+ communities stated that they did not report TFGBV violence to the police due to an awareness of discriminatory legal processes and to avoid the risk of facing incrimination. A respondent shared a case where hesitancy to report an incident to the police was coupled with the risk that the victim would face accusations of defamation. Other respondents relayed that some of those relying on legislative protections found that, by default, those protections turned the incrimination back on them.

85 United Nations, Office for Disarmament Affairs, UN Security Council Open Debate on Cyber Security: Maintaining International Peace and Security in Cyberspace, June 29, 2021.
86 The Centre for Feminist Foreign Policy (CFFP) (2023). *Policy Brief ¬– Feminist Perspectives on the Militarisation of Cyberspace*. https://centreforfeministforeignpolicy.org/2023/06/21/feminist-perspectives-on-the-militarisation-of-cyberspace/
87 The Philippines Commission on Women works closely with the ASEAN commission to advocate many cross-cutting issues.
88 Congress of the Philippines (2018). REPUBLIC ACT No. 11313 - An Act Defining Gender-Based Sexual Harassment in Streets, Public Spaces, Online, Workplaces, and Educational or Training Institutions, Providing Protective Measures and Prescribing Penalties Therefor, https://lawphil.net/statutes/repacts/ra2019/ra_11313_2019.html
89 Valerio Loi, *Defending in Numbers 2019-2020* (Forum Asia: 2021). https://www.forum-asia.org/uploads/wp/2021/06/Defending-in-Numbers-A-Message-of-Strength-from-the-Ground-for-web.pdf
90 Nermine Aboulex, *The Chilling: Global Trends in Online Violence against Women Journalists* (UNESCO, 2021). https://unesdoc.unesco.org/ark:/48223/pf0000377223
91 International Commission of Jurists (2019). *Dictating the Internet: Curtailing Free Expression, Opinion and Information Online in Southeast Asia*. https://www.icj.org/southeast-asia-icj-launches-report-on-increasing-restrictions-on-online-speech/

4.4. Lack of Diverse Perspectives in Decision-Making

The critical underrepresentation of women in digital security and tech positions, as well as decision-making at large, further compounds the lack of gender considerations in these spaces. It is estimated that women make up only 25 per cent of the world's cybersecurity professionals, with a smaller percentage holding senior leadership positions.[92]

Moreover, the digital gender gap — where women are less likely than men to have an online presence — is pervasive. In 2023, the digital gender gap in the Asia-Pacific region stood at six per cent, with 63 per cent of women in the region using the Internet compared to 69 per cent of the region's men.[93] These gaps can, among other factors, be explained by different social norms and expectations, whether women have the right to freely own and use online communication devices, and by the costs of connectivity and income disparities between women and men, where women may be less likely to afford devices or access.

Respondents voiced challenges pertaining to the digital gender gap, pointing out that having fewer women engaged in decision-making processes reduces the likelihood that gender will feature as a topic. Respondents also explained that with fewer women being digitally connected, their opportunities to develop digital skills and literacy are significantly reduced. In turn, this is having negative impacts on their digital security practices, making them more vulnerable to TFGBV and cyberattacks at large.

Respondents stressed that inequitable Internet access is an intersectional issue. While gender identity and expression are explanatory factors, they interplay with other factors such as age, sexual orientation, socioeconomic status, ability status and geographic location. For example, the extent to which people with diverse SOGIESC can freely express their identities differs across countries in the region. Extensive censorship on diverse SOGIESC and self-censorship within the community was observed in countries where LGBTIQ+ communities are particularly stigmatized. [94]

> *"Social status is a barrier in accessing the Internet. In our university, we have classmates from places where they don't have Internet access. What they do is go up the mountains to get Internet signal or connection. It is really difficult for them and they are located in isolated places.*
>
> – Woman student, South-East Asia

At a focus group discussion held in Indonesia, two women with disabilities said that they faced more difficulties than others when using social media. They cited barriers such as the paucity of accessible technology and insufficient linguistic assistance for people with different needs (e.g. the availability of subtitles or sign language options). While the two informants acknowledge the benefits of digital access, they also reported being exposed to online harms due to their disabilities.

92 Cybersecurity Ventures (2022). *Women in Cybersecurity 2022 Report*. https://cybersecurityventures.com/wp-content/uploads/2022/09/Women-In-Cybersecurity-2022-Report-Final.pdf
93 ITU (2023). Measuring Digital Development – Facts and Figures 2023. https://www.itu.int/hub/publication/d-ind-ict_mdd-2023-1/
94 OutRight Action International, The Citizen Lab, and Open Observatory of Network Interference (OONI), *No Access: LGBTIQ Website Censorship in Six Countries* (2021). https://citizenlab.ca/wp-content/uploads/2021/08/LGBTIQ-censorship-Final-1.pdf

5.

CONCLUSION: A WAY FORWARD FOR WOMEN, PEACE AND DIGITAL SECURITY

Women and women leaders in South-East Asia face diverse online harms. While conveyed in a number of different ways, the systematic nature of online attacks to silence women's voices and to discredit their work poses a significant obstacle to advancing gender equality, human rights and inclusive peace across the region. Concerted efforts are required to address these issues, ensuring that adequate protection and recovery services are readily available and, more importantly, to prevent incidences of TFGBV, the normalization of TFGBV, and attempts to suppress online freedom of speech and expression. As the WPS agenda evolves to respond to imminent changes in the world we live in, its principles provide a foundation to advance safe and inclusive digital spaces while positioning women's leadership at the centre of change-making processes. Given that the digital world permeates all sectors of society, efforts to mainstream key principles of the agenda across digital governance systems will depend on multisectoral dialogues and collaborative efforts among national and international stakeholders.

5.1. Recommendations

Recommendation 1: Undertake holistic and evidence-based strategies to effectively prevent, counter and respond to incidences of TFGBV, particularly in politically volatile and conflict- and crisis-impacted contexts.

a. **Develop strategies to tackle misogynistic content on digital platforms, including gendered hate speech, disinformation and violent and extremist messaging, through improved accountability mechanisms across the public and private sectors**, ensuring that human rights commitments, including freedom of speech, expression and assembly, are adhered to.

b. Invest in greater efforts to prevent and respond to the spread of gender-based digital security threats through the **review and reformulation of existing company policies, automated content management algorithms and other forms of artificial intelligence** in order to account for bias and discrimination based on gender, age, ethnicity and other relevant factors.

c. **Develop and strengthen existing TFGBV early warning and response mechanisms in conflict- and crisis-affected settings** to quickly detect and counter the spread of hate speech, misogyny and false or misleading information and harmful behaviour.

d. **Conduct regular and context-specific assessments of the digital landscape, disaggregated by sex, age and other relevant factors**, in order to inform evidence-based policy formulation in digital security planning, design, governance and enforcement without infringing on personal integrity or compromising privacy concerns.

e. **Provide stable, reliable and affordable Internet connectivity, with particular attention given to intersectionality and bridging the digital gender divide**. This can be achieved by expanding critical infrastructure and broadband connectivity, especially in rural and other areas with lower Internet access, ensuring that women, young women, and girls in all their diversity benefit equally from these investments. This also includes avoiding practices such as Internet shutdowns, broadband throttling and other means of hindering or slowing Internet access.

Recommendation 2: Advance knowledge, capacities and tools to ensure that women and persons with diverse SOGIESC can safely and equitably lead the development and governance of ICTs and digital platforms, including advancing online civic engagement and digital peacebuilding.

a. **Provide digital literacy and digital safety programming** for women in all their diversity, including through self-paced learning, campaigns and outreach, to raise awareness of gendered digital harms and to mitigate the impacts of harmful online content.

b. **Integrate digital rights curricula in schools and universities**, focusing on the appropriate uses of the Internet, social norms, and the prevention of digital harms that may spur conflict, social tensions and other types of harm.

c. Undertake tangible measures, including **providing financial support to digital rights organizations and local women's groups**, in order to reach and enhance the digital literacy and cyber resilience of marginalized women, women living with disabilities, and LGBTIQ+ groups.

Recommendation 3: Ensure that cyber- and digital security laws, policies and strategies are gender-responsive, informed by principles underlying the WPS agenda, and adherent to international law and human rights obligations.

a. **Integrate digital security-related considerations in the design, implementation and evaluation of regional and national action plans on WPS** and other related policy frameworks, ensuring that there are dedicated budgets and high-quality mechanisms for monitoring the implementation of priorities that sit in the intersection between digital security and international, national and human security.

b. **Prioritize harmonizing existing laws and legislation related to digital spaces, gender equality and human rights.** These should adhere to, and diligently uphold, basic human rights principles.

c. **Ensure that privacy protection policies and data collection and storage practices are transparent**. Ensure that the public, particularly women and marginalized communities who may face greater barriers in engaging with key decision-makers, has opportunities and avenues to voice concerns regarding data management and that they can request the deletion of all data collected on them.

d. Hold governments, digital companies, and international actors accountable for **addressing online human rights issues through gendered approaches and by developing gender-responsive and locally grounded cybersecurity tools** that are accessible to the public and account for users with diverse needs and language requirements.

ANNEX 1.

METHODOLOGY OF INITIAL STUDY LED BY INSAAN CONSULTING LTD.

This report is part of a broader qualitative study conducted by Insaan Consulting that explored Internet user experiences in South-East Asia through a gender lens with a focus on four areas: Internet access and user profiles, cyber-harms, recourse to justice and opportunities and challenges for positive online engagement for peace and social cohesion. For this study, Insaan Consulting Ltd. collected data from May to October 2021 via interviews and focus groups with a concentration on 10 South-East Asian countries.[95] The study informants (predominantly women) were selected with the help of three key gender specialists, one based in the Philippines and two in Indonesia. To ensure a diverse sample when selecting interview and focus group participants, the specialists considered gender, age, religion, ethnicity, socioeconomic status, geography and involvement in advocacy work.[96]

In the broader study, 40 respondents participated in online interviews, and 44 respondents joined the five focus group discussions (four of which were held online due to COVID-19 restrictions). The respondents were either based in or working on issues in Brunei, Cambodia, India, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Thailand, Singapore, the United States and Viet Nam. Respondents included women in politics; activists focused on areas including climate change, feminism and political and social rights; human rights defenders; digital rights organizations; CSOs and NGOs; women's organization employees and affiliates; women engaged in business, e-commerce, financial technology and start-ups; academics; lawyers; a pop star; think tanks; and regional organizations. To protect the respondent' anonymity and to avoid placing them at risk, their accounts are presented with reference to their background rather than their names.

Interview duration and content were adjusted based on individual respondents' willingness and comfort to speak about certain sensitive subjects and questions. In addition, respondents were given the option to keep their cameras on or off during the interviews.

In Indonesia, 26 total participants from Bantul, Poso, Sleman, Surakarta, and Yogyakarta participated in three focus group discussions. The participants included 12 women student representatives; 10 representatives from women's organizations, CSOs and beneficiaries; and four individuals with diverse SOGIESC. In the Philippines, 18 total participants from Baguio, Cavite, Cebu, Iloilo, Laguna and the National Capital Region participated in two focus group discussions.

Academics from Indonesia and the Philippines with experience working with survivors of online harms (predominantly women and people with diverse SOGIESC) facilitated the focus group discussions. These academics were equipped to take necessary safeguards during and after the interview processes and to provide support for specific needs when required.

The interview and focus group questions primarily concentrated on four areas: access and usage profiles, concerns and harms, recourse and knowledge on protections, and opportunities to ensure gender-inclusive cybersecurity practices. The interview and focus group questions informed the coding and categorization of the collected data (including the nature of the questions), which facilitated analysis. Analysis results were reviewed by three experts who were not involved in the coding or analysis processes. The broader study's preliminary findings were shared in a webinar; relevant feedback was incorporated into this report.

95 Brunei, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Viet Nam.
96 Interviews and focus groups encompassed the participation of 70 women and 14 men, including four individuals identifying as people with diverse SOGIESC. Two informants identified as living with disability.

Data collection limitations and challenges include pandemic-related constraints on time and physical meetings; some countries' and individuals' sensitivity to the discussion topics; the coup d'état in Myanmar; logistical arrangements that had to be made in Indonesia (the study corresponded to the Ramadan period); and language and access-related barriers, especially in countries such as Cambodia and Lao PDR.

This report focuses on gendered online harms, access and participation-related issues that emerged from the broader study and evaluates that study's findings through a WPS lens, including analysis of the WPS pillars of meaningful participation, prevention and protection. It also continues the broader study's efforts to map regional legal and policy initiatives against cyber threats. In this current report, the broader report's interview and focus group findings are coupled with a literature review on relevant topics. The literature review involved analysing relevant global and regional reports (including those from UN Women and ICT industries), digitally accessed data sets, media coverage and online content relevant to respondent discussions.

In June 2022, inputs for this report were requested from 19 CSOs in South-East Asia during a three-day workshop organized in Bangkok, Thailand, by the UN Women Regional Office for Asia and the Pacific. The CSO representatives provided their views on the findings and shared additional insights to address gaps identified during the workshop; the report was subsequently revised to reflect these inputs. CSO representatives reviewed and verified added points as they were incorporated into the report.

BOX 1. METHODOLOGY

44 students, women's organization staff, survivors of violence and individuals with diverse SOGIESC participated in focus group discussions in urban and rural areas of Indonesia and the Philippines.

40 key informant interviews were conducted with politicians, activists, human rights defenders, digital rights organizations, CSOs, NGOs, women-led organizations, academics, businesswomen in e-commerce and financial technology, lawyers, public figures, think tanks and regional organizations across the 10 South-East Asian countries.

Participations of the study interviews and focus groups together saw the participation of 70 women and 14 men, including four individuals identifying as people with diverse SOGIESC and two respondents identifying as living with a disability.

Findings were presented to 19 national and regional CSOs from South-East Asia at a three-day workshop in June 2022. The resulting insights were incorporated into this report.

Primary data was supplemented by a literature review of relevant media, statistics and global sources in the areas of cybersecurity and WPS.

ANNEX 2.

OVERVIEW OF UNSC DIALOGUES ADDRESSING DIGITAL SECURITY

DATE	TYPE	SUBJECT	ORGANIZER(S)
26 Nov 2016	Arria-formula	Cybersecurity and international peace and security	Senegal, Spain
31 Mar 2017	Arria-formula	Hybrid wars as a threat to international peace and security	Ukraine
22 May 2020	Arria-formula	Cyber stability, conflict prevention and capacity building	Estonia
26 Aug 2020	Arria-formula	Cyber-attacks against critical infrastructure	Indonesia
2 Oct 2020	Arria-formula	Access to education in conflict and post-conflict contexts: Roles of digital technology and connectivity	Belgium, China, Dominican Republic, Estonia, France, Germany, Niger, St. Vincent and the Grenadines, South Africa
12 May 2021	Arria-formula	Delivering accountability through innovation and partnership: Harnessing technology to deliver justice for war crimes, crimes against humanity and genocide	United Kingdom, Iraq, United States
17 May 2021	Arria-formula	The Impact of Emerging Technologies on International Peace and Security	China
29 June 2021	**UNSC open debate**	**UNSC High-Level Open Debate on Cyber Security – Maintaining international peace and security in cyberspace**	**Estonia**

DATE	TYPE	SUBJECT	ORGANIZER(S)
28 Oct 2021	Arria-formula	Addressing and countering hate speech and preventing incitement to discrimination, hostility and violence on social media	Kenya
20 Dec 2021	Arria-formula	Preventing civilian impact of malicious cyber activities	Estonia, United Kingdom
25 May 2023	Arria-formula	The responsibility and responsiveness of states to cyber-attacks and critical infrastructure	Albania, United States
18 Jul 2023	**UNSC open debate**	**UNSC High-Level Open Debate on Artificial Intelligence**	**United Kingdom**
19 Dec 2023	Arria-formula	Artificial intelligence and its impact on hate speech, disinformation and misinformation in the context of the maintenance of international peace and security	United Arab Emirates, Albania

Source: United Nations Security Council Arria-Formula Meetings Dashboard[97]

97 United Nations Security Council. *Arria-Formua Meetings Dashboard.* https://www.un.org/securitycouncil/content/repertoire/research-tools/Arria-formula

Research supported by

Ministry of Gender Equality and Family

Australian Government

CYBER & CRITICAL TECH COOPERATION PROGRAM

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

June 2024