Introduction

Providing a more holistic and inclusive security framework (as stipulated by the United Nations Security Council Resolution 1325 and subsequent resolutions) entails doing more to integrate cybersecurity considerations into the Women, Peace and Security (WPS) agenda. Achieving context-specific, conflict-sensitive and gender-responsive cybersecurity will require adopting a WPS lens when making and operationalizing policy decisions related to online and offline spaces, particularly those concerning peacebuilding and conflict resolution.

A WPS lens would include:

Participation and representation
Ensuring and promoting women’s leadership, participation and representation in technology and cybersecurity planning, design and governance and relevant law enforcement efforts, in line with WPS recommendation.

Prevention
Preventing gender-based cybersecurity threats, online harms and cyber-enabled crimes through conflict-sensitive and gender-responsive approaches.

Protection of rights
Protecting women’s human and digital rights while ensuring their safety from gender-based cybersecurity threats, online harms and cyber-enabled crimes, both online and offline.

Relief and recovery
Relief and recovery efforts in post-conflict/crisis contexts should use technology in a conflict-sensitive, gender-responsive and survivor-centred manner.
This advocacy brief was developed by representatives from women’s civil society organizations (CSOs), digital rights organizations, think tanks, academia and cyber-defenders in Southeast Asia, with the support of UN Women. The brief emphasizes the importance of cybersecurity and its gendered implications for implementing the WPS agenda. In developing this brief, the collective was guided by principles of gender equality, diversity and inclusion.1

This brief is intended for ASEAN Member States, ASEAN and other intergovernmental bodies, cybersecurity and digital security expert groups, digital companies and CSOs. It offers best approaches to ensuring that cybersecurity concerns are considered in efforts to implement the WPS agenda while introducing gender-responsive measures into the broad spectrum of cybersecurity. These approaches are based on international legal and normative human rights frameworks and WPS principles.

Participation and Representation

Ensuring and promoting women’s leadership, participation and representation in technology and cybersecurity planning, design, governance and in law enforcement efforts in line with WPS recommendations.

When compared to other regions across the globe, Southeast Asia has the highest share of women in the tech workforce. However, when compared to other industries, women’s representation in technology remains low.2 Women’s underrepresentation in technology fields and related decision- and policy-making has led to gender-biased technology planning, development and utilization. Further, these areas and surrounding regulations tend to be gender-blind, generally lacking considerations of gendered implications and overlooking women’s perspectives.

To rectify these shortcomings when developing governance and operational aspects of cybersecurity, ASEAN Member States and other relevant actors should undertake inclusive consultations with cybersecurity experts, gender experts, women’s groups, youth, persons with disabilities, persons with diverse sexual orientation, gender identity, gender expression and sex characteristics (SOGIESC), Indigenous peoples, and other marginalized groups. Such consultations should also include private-sector entities, including but not limited to digital platforms and social media companies.

Relevant actors should:

• Ensure women’s leadership and guarantee their genuine and meaningful participation in the planning, design and governance of technology and cybersecurity;

• Collect data segregated along the lines of sex, age, gender, disabilities, socioeconomic and other relevant factors to inform context-specific and conflict-sensitive policy formulation;

• Review and amend laws and policies concerning cyber-enabled crimes, cybersecurity, data breaches, that are harmful to women and marginalized groups, and enforce laws, policies, cyber-incident response teams and e-forensics that advance gender equality and transformation in cyberspace;

• Ensure women’s leadership and meaningful participation in developing and formulating cybersecurity of policies and laws;

• Promote women’s participation of women in cybersecurity-related law enforcement (e.g. cybercrime investigations); and

• Lead and support online peacebuilding efforts by providing digital safe spaces in order to encourage dialogue, repair relationships, reform institutions and address the socioeconomic dimensions of conflict and obstacles to social cohesion.

Prevention

Preventing gender-based cybersecurity threats, online harms and cyber-enabled crimes through conflict-sensitive and gender-responsive approaches

Responses to the gendered dimensions of cyber-enabled crime and online harms are fundamental aspects of the WPS agenda, which aims to create and sustain inclusive, holistic security. Preventing gender-based cybersecurity threats,

1. While the word women is used as a reference throughout this document, the advocacy brief concerns not only women, but also girls and people with diverse sexual orientation, gender identity, gender expression and sex characteristics.

harms and cyber-enabled crimes is significant to the WPS agenda and requires tailored solutions. However, this thematic field remains understudied, and, to date, there are few substantive tools and resources to redress this challenge.

ASEAN Member States and other relevant actors, including but not limited to intergovernmental bodies, digital companies, cybersecurity and digital security expert groups and CSOs should:

• Integrate digital literacy and cybersecurity as part of the regional WPS agenda and the early education curriculum to reach young women, men and persons with diverse SOGIESC;

• Prevent the spread of gender-based cybersecurity threats, harms and cyber-enabled crimes through the formulation and implementation of policies and laws that mitigate these risks;

• Strengthen and diversify existing oversight, early warning and response mechanisms related to online harms, including responses to gendered, violent and misogynistic narratives, disinformation or otherwise harmful content;

• Support CSOs, women human rights defenders, women in politics and women journalists to build capacities and support communities to raise awareness and promote risk-mitigation strategies on cybersecurity threats, harms and cyber-enabled crimes;

• Enhance governments’ and relevant stakeholders’ public transparency on privacy protection policies and in all forms of digital activities in compliance with conflict-sensitive, gender-responsive and rights-based principles. This includes the prevention of the use of technology and digital platforms to, in an adverse manner, track or profile women and marginalized groups such as refugees/internally displaced persons and other relevant groups, with a specific focus on conflict, post-conflict and other contexts with heightened insecurity;

• Ensure that the population has equal and secure access to correct, verifiable and updated information on their digital rights, privacy considerations and gender-responsive principles that take account of cybersecurity threats and harms and the specific needs, challenges and vulnerable situations of women, girls and people with diverse SOGIESC characteristics; and

• Make information, training and guidance on good cybersecurity practices widely available in Southeast Asian languages to help CSOs and other actors assess their operational and programmatic risks, prevent cyberattacks and increase their knowledge of and response to cyber incidents when faced with conflict risks such as hate speech and disinformation.

Protection of Rights

Despite the opportunities it offers, the Internet also generates gender-based cybersecurity threats, harms and cyber-enabled online and offline crimes.

Protecting women’s human and digital rights while ensuring their safety from gender-based cybersecurity threats, online harms and cyber-enabled online and offline crimes.

• Encourage the identification, further formulation and regular progress assessment of regional and national gender-responsive and rights-based standards to address gendered cyberthreats, harms and cyber-enabled crimes (e.g. the ASEAN Regional Plan of Action on Women, Peace and Security and other relevant regional and national action plans);

• Protect women from online attacks and their repercussions, with specific attention to women human rights defenders, journalists and politicians who face harm, and ensure that the protection mechanisms available for offline harm also apply to online spaces;

• Ensure that laws and policies take gendered cyberthreats, harms and cyber-enabled crimes into account. Laws and policies should be drafted in a language that is understandable by impacted stakeholders, that addresses the issues and that keeps up with technological developments and emerging threats and harms;

• Equip law enforcement agencies and the judiciary with the capacity to provide protection and to implement relevant laws and policies on cyberthreats, harms and cyber-enabled crimes in a conflict-sensitive, gender-responsive and survivor-centred manner. This includes developing mechanisms and capabilities such as e-forensics and other relevant investigation methods;
• Ensure transparent and accountable governance mechanisms that facilitate coordination among national and local governments, security actors and digital platforms in order to strengthen the protection of women’s human and digital rights;

• Guarantee that the mechanisms that government and non-government actors and private-sector businesses use to collect, use, store and manage digital data comprehensively protect personal information and minimize the risks of gendered rights violations;

• Ensure that digital companies are accountable for proactively addressing threats and harms, including through the removal of private data and harmful information from the Internet. Ensure that these companies maintain clearly identified and accessible contact points for users and law enforcement; and

• Ensure that sufficient and sustainable resources are specifically budgeted and allocated to the improvement of regional protection mechanisms to safeguard CSOs, women rights defenders, women journalists and women politicians from cybersecurity threats, online harms and cyber-enabled crimes.

Relief and Recovery

Relief and recovery efforts in post-conflict/crisis contexts should use technology in a conflict-sensitive, gender-responsive and survivor-centred manner.

In post-conflict situations, technology can support relief, recovery and peacebuilding efforts if used in a conflict-sensitive, gender-responsive and survivor-centred manner. Maintaining safe and sound cybersecurity practices is an important tool to foster relief and recovery from the cybersecurity threats, online harms and cyber-enabled crimes that happen during conflicts and crises. ASEAN Member States and other relevant actors, including but not limited to intergovernmental bodies, digital companies, cybersecurity and digital security expert groups and CSOs should:

• Support safe online peacebuilding efforts by women’s CSOs and movements in post-crisis and conflict contexts in relief and recovery efforts that sustain peace efforts, including those efforts that address online threats and harms to peace and security;

• Ensure that high-quality and gender-responsive relief and recovery support is provided to persons and communities that have suffered increased risks to their personal security and well-being, reprisals or have been otherwise negatively affected by hacking, data breaches or other cyber-facilitated malicious acts during conflict and crises;

• Promote and support the development of disaster recovery plans that outline strategies for recovery crisis management, business continuity and impact assessment, thus ensuring that organizations, networks and civil movements, government bodies, institutions and public services that are working to support survivors of conflict-related harms and abuses and to provide economic relief, healthcare and psychosocial support to survivors of conflict-related harms and abuses are able to quickly resume operations after being exposed to cyber-attacks. Such disaster recovery plans and strategies will ensure the swift continuation and maintenance of relief and recovery efforts, particularly for women and young women; and

• Develop and ensure that existing public cybersecurity responses to large-scale cyber-enabled crimes go beyond providing support to large entities; responses should also support small-scale claims and relief and recovery efforts aimed at the individual level with a conflict-sensitive, gender-responsive and people-centred approach.