WHY IS CYBERSECURITY RELEVANT TO THE WOMEN, PEACE AND SECURITY AGENDA?

Cybersecurity is an increasingly recognized priority area for international and national security policies; its prominence has grown in parallel with the accelerated rate of digitalization that has also stemmed from COVID-19 pandemic response measures. Emerging technologies, cyberwarfare and attacks on critical infrastructure are becoming the norm in today’s armed conflicts and defence operations.1 While the Internet has opened up a broad spectrum of venues for civic engagement, digital peacebuilding and activism — particularly for women, young women and marginalized groups who have struggled to access traditional public platforms and decision-making spaces — strict surveillance, Internet shutdowns and bandwidth throttling have become commonplace in curtailing freedom of expression and assembly and resulting in shrinking civic spaces across the Asia-Pacific region.

Along with the potential for more accessible information, rapid communication and platform building, digital platforms are increasingly used to spread disinformation, hate-speech, misogynistic and radicalizing content, heighten “echo chambers” and to facilitate illicit activities such as trafficking and sexual exploitation, which disproportionately affect women. Moreover, the experiences of women’s civil society organizations (CSOs), women human rights defenders, women politicians and other public figures across Southeast Asia have shed light on the increasing use of harmful tactics such as cyberbullying, trolling and doxing to silence and discredit voices and engagement that favours gender equality and women’s rights. Given the critical underrepresentation of women in leadership and decision-making spaces related to cybersecurity, technology development and peacebuilding at large, measures taken to mitigate the gendered implications of these risks are lagging behind.2

This project is part of the UN Women Regional Office for Asia and the Pacific Regional Framework Towards Peaceful, Inclusive Societies: Advancing the Women, Peace and Security Agenda and Inclusive Governance in the Asia Pacific Region. Cybersecurity is recognized as a key emerging issue under the framework, and the programme falls under both its pillars; Pillar 1 – Women, Peace and Security, and Pillar 2 – Inclusive Governance.
The Women, Peace and Security agenda recognizes the multiple roles that women have in conflict situations and in peace efforts. Since its adoption over two decades ago, much has happened to the global playing field, and non-traditional security issues - including cybersecurity - are increasingly relevant to international peace and security. In recognition of the implications that technology and cybersecurity have on current security challenges, UN Women recommends the following measures:

1. **Participation**
   - Strengthen women’s leadership and meaningful participation in cyber-related legislation, decision-making and enforcement and in the development, audit and governance of contemporary and emerging technologies in line with the women, peace and security principles.

2. **Prevention**
   - Leverage conflict-sensitive and gender-responsive approaches to detect and prevent the gendered impacts of digital security threats, harms and crimes facilitated by information and communications technologies (ICTs) as well as to avoid disruptive Internet shutdowns and blocking that impact on women’s security.

3. **Protection**
   - Safeguard the human rights, physical safety and mental well-being of persons in all their diversity, with specific attention to the disproportionate risks of being exposed to ICT-facilitated harms and crimes that women experience (particularly women journalists, activists, human rights defenders, politicians and other public figures), particularly in conflict, post-conflict and crisis contexts.

4. **Relief and recovery**
   - Utilize the positive potential of deploying context-specific, rights-based and gender-responsive technological solutions to enhance and expand the reach of relief and recovery efforts in post-conflict and post-crisis contexts.
PROGRAMMATIC APPROACH

With generous support from the Government of the Republic of Korea and the Australian Department for Foreign Affairs and Trade, UN Women is implementing the Women, Peace and Cybersecurity: Promoting Women’s Peace and Security in the Digital World programme. The programme aims to promote the Women, Peace and Security agenda to ensure that women, including young women, lead and participate at all levels of ICT policy and decision-making, while contributing to the implementation of UN Women’s Regional Framework Towards Peaceful, Inclusive Societies: Advancing the Women, Peace and Security Agenda and Inclusive Governance in the Asia Pacific Region. The programme will integrate the following strategies:

Overarching strategies

» Design strategic approaches for conflict-sensitive and gender-responsive digital security through evidence-based and consultative methods;

» Enhance digital literacy, awareness and sound cybersecurity practices for women in all their diversity;

» Support multisectoral advocacy and leverage governments’ and private sector actors’ support for conflict-sensitive and gender-responsive digital security; and

» Engage in whole-of-society legal and policy reform that strives to harmonize cybersecurity, national security and international security frameworks.

Through these strategies, UN Women is currently working on the following programmatic areas:

Promoting women’s leadership in cybersecurity

The digital world and its governing structures are complex and rest on a foundation of numerous actors, including governments, digital media companies and a range of private-sector actors. Women’s voices are underrepresented in politics, negotiation panels, company boards and across all Science, Technology, Engineering, Math (STEM) fields. UN Women is working to create multi-stakeholder platforms for women’s civil society representatives and subject-matter experts to influence the design, audit and governance of technologies, digital platforms and cybersecurity-related areas to accelerate momentum for gender-responsive approaches to gendered security challenges in the digital age.

Supporting conflict-sensitive and gender-responsive cybersecurity legal and policy reform

While most states have adopted cybersecurity-related laws, strategies and policies, very few have included gender provisions or recognised the disproportionate impacts that online harms, threats and ICT-facilitated crimes have on women. UN Women has conducted a mapping of cyber-related laws and policies across the region and consulted with women’s CSOs, think tanks, and young cyberdefenders on cybersecurity priorities for the region. UN Women is currently developing policy recommendations based on this research.vi

UN Women is working closely with governments in the region, with a specific focus on the Philippines, Thailand and Viet Nam, to advance a more conflict-sensitive and gender-responsive cybersecurity agenda. UN Women is also providing technical inputs and advocating for conflict-sensitive and gender-responsive cybersecurity approaches in the development of the ASEAN Regional Plan of Action for Women, Peace and Security.

Analysing threats and obstacles to women’s online civic engagement and peace efforts to develop evidence-based countermeasures

Milestone research conducted by UN Women on the cybersecurity implications of implementing the Women, Peace and Security agenda in Southeast Asia showed that harmful online acts’ result in self-censorship and unwarranted political scrutiny.vii UN Women is analysing and raising awareness on the gendered dynamics and impacts of these harms to better inform policy reform and to enhance prevention, response and recovery efforts for ICT-facilitated harms and crimes.

1. UN Women’s research found that Internet users across Southeast Asia identified cyberbullying, trolling, doxing, outing, hate-speech and disinformation as key obstacles to women’s peacebuilding and civic engagement, in addition to systematic surveillance, Internet shutdowns and bandwidth throttling.
Combating disinformation, misogynistic hate-speech and violent extremism

Along with the increasing degree of connectivity across the Asia-Pacific region and globally, disinformation and violent and radicalizing narratives are spreading rapidly. Misogynistic hate speech is on the rise. According to research conducted by UN Women in 2020, misogyny and support for violence against women closely relate to the narratives and recruitment strategies of violent extremist groups. UN Women is also building the capacities of law and women human rights defenders to identify key needs to address these trends and to develop peaceful counter-narratives.

Understanding gendered security implications of emerging technologies and artificial intelligence while employing them for inclusive peace

Artificial intelligence (AI) is increasingly used in surveillance and military technologies and constitutes the foundation of everyday technologies, from online search functions to social media platforms. Several studies have indicated that AI-powered systems host and reinforce gender and racial biases, which disadvantage women and women of colour in particular. UN Women is conducting research on gendered security risks related to AI and emerging technologies and identifying opportunities to employ such technologies for inclusive peace.

Strengthening the capacities and resilience of women to stay safe from and to combat cyber-enabled crimes and technological vulnerabilities

While communities are rapidly becoming more connected, digital literacy is lagging behind, particularly for elderly, rural and Indigenous women, resulting in higher risks of being exposed to ICT-facilitated harms and crimes. Further, digital platforms are increasingly being used to facilitate exploitation and transnational crimes such as human trafficking. Transnational criminal networks and other malevolent actors are also engaging in hacking, phishing and the spread of ransomware to access personal data. Being exposed to these offences is particularly risky for women human rights defenders and other stakeholders who work with sensitive data and information. UN Women is working on mapping positive examples of digital peacebuilding in the region in order to enhance the understanding of opportunities that technology has for women in peace efforts across the region, and to expand the establishment of intra and inter-regional Women, Peace and Security platforms and movements.

Strengthening the capacities of women peacebuilders to use digital tools for peacebuilding

Technology can make positive contribution to peacebuilding processes by offering tools that foster collaboration, raise awareness, transform attitudes, and give a stronger voice to communities. Although peacebuilders are becoming increasingly reliant on digital platforms and technological solutions to leverage their work, gendered online harms and gender biases in technologies hinder women’s online peacebuilding efforts. UN Women is working closely with women’s CSOs and women human rights defenders to identify key needs and means of strengthening their cybersecurity practices and resilience. UN Women is also building the capacities of law enforcement bodies to address these security risks.
WHERE WE WORK

The Women, Peace and Cybersecurity – Promoting Women’s Peace and Security in the Digital World programme is currently implemented regionally in Southeast Asia, with country-level activities in the Philippines, Thailand and Viet Nam. The results and best practices from the programme will be used for advocacy purposes to influence policy-making elsewhere in the Asia-Pacific region.

FORWARD-LOOKING PRIORITIES

In addition to the aforementioned initiatives, UN Women envisions closer engagement under the following intervention areas:

- **Gender-responsive cybersecurity under international law and principles**

Although states that are part of the Open-Ended Working Group on security in the use of information and communication technologies have affirmed that international law “is applicable and essential to maintaining peace, security and stability in the ICT environment,” there is still little consensus as to how international law should be applied to cybersecurity concerns.xii

Nevertheless, numerous ongoing initiatives are attempting to fill this gap. A comprehensive international convention on countering the use of information and communications technologies for criminal purposes is currently underway.xiii In addition, the UN Group of Governmental Experts on advancing responsible state behaviour in the context of international security have launched 11 non-binding, voluntary norms of responsible state behaviour in cyberspace; numerous countries have adopted these norms. However, because these discussions and norms lack a gender perspective,xiv there is a need to develop conflict-sensitive and gender-responsive recommendations in these areas, while localizing them to contexts across the Asia and the Pacific region.
Women’s participation in cyberdiplomacy and cybersecurity negotiations

The representation of women diplomats engaged in cyber-related topics is among the lowest across all groups.¹⁵ UN Women stresses the importance of supporting women’s (particularly young women’s) negotiators’ and cyberdefenders’ access to high-level decision-making spaces, and will continue to strengthen the capacities of women-led negotiator networks to advocate for locally grounded, conflict-sensitive and gender-responsive cybersecurity. More efforts to support women’s digital peacebuilding in conflict- and crisis-affected countries are also needed.

Expanding Women, Peace and Cybersecurity efforts to South Asia and the Pacific

The peace and security context across the Asia-Pacific region is diverse, particularly in terms of cybersecurity, with countries in the Pacific and parts of South Asia having a low degree of connectivity compared to the relatively high degree of digitalization across societies in Southeast Asia. Nevertheless, cybersecurity is a critical issue in countries with a lower degree of connectivity, such as Afghanistan, Myanmar, Solomon Islands and Sri Lanka, and for CSOs operating in similar contexts. In order to address the full spectrum of gendered cybersecurity issues across the entirety of the Asia-Pacific region, UN Women is seeking to expand the geographic scope of the programme beyond Southeast Asia.

For more information, please contact:

**Gaëlle Demolis Ebassa**
Governance, Peace and Security Specialist
UN Women Regional Office for Asia and the Pacific
gaëlle.demolis@unwomen.org

**Alexandra Håkansson Schmidt**
Governance, Peace and Security Analyst
UN Women Regional Office for Asia and the Pacific
alexandra.hakansson@unwomen.org

Women learning robotics in Bangkok, Thailand, 02 April 2022. - Photo: UN Women/Ana Norman Bermudez
REFERENCES


vii Ibid.


xii https://digitallibrary.un.org/record/3984905?ln=en

xiii A/RES/74/247

xiv A/70/174