ACTION BRIEF

WOMEN, PEACE & (CYBER) SECURITY IN ASIA AND THE PACIFIC

WOMEN, PEACE & (CYBER) SECURITY: COVID-19 AND BEYOND

Among the urgent challenges to peace and security posed by the COVID-19 pandemic, cybersecurity has emerged as a new and critical area for the application of the Women, Peace and Security (WPS) agenda in Asia and the Pacific.

Technological innovation can play a key role in building and sustaining peace. Information and communication technology (ICTs) have opened new ways for preventing conflict and increasing civic engagement. Transformative technologies have enabled high-speed early warning systems, geographic information systems to track conflicts, platforms for inclusive and consultative peace processes, and empowered citizens to counter the spread of misinformation. These advancements are all underpinned by cybersecurity.

The COVID-19 pandemic has highlighted how advancements in the digital world can be leveraged to respond to threats to peace and security, with governments, technology companies, international organisations, and civil society alike announcing digital solutions to understand and respond to the pandemic.

The pandemic has also demonstrated that digital solutions must be supported by strong cybersecurity frameworks. From cyberattacks on hospitals, medical research facilities, and other essential infrastructure, to malware in fake World Health Organisation (WHO) information apps, to phishing emails offering personal protective equipment, and digital surveillance and contact tracing, COVID-19 has placed cybersecurity front and center of current peace and security discussions, including by the Security Council, and highlighted the next frontier for the WPS agenda.

Massive cyberattacks could well become the first step in the next major war.

United Nations Secretary-General (S/2018/404)

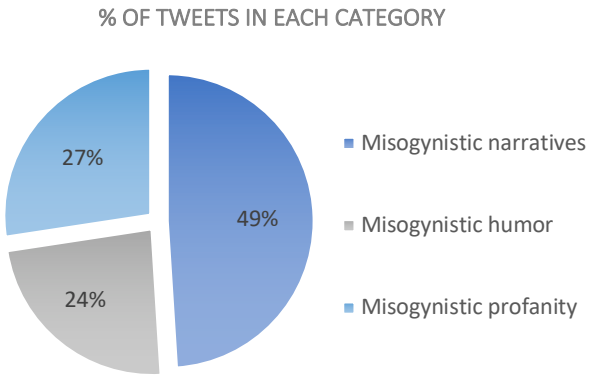
DIGITAL HARMS TO WOMEN AND GIRLS

As governments, industry, and technology companies invest in strengthening digitisation, and make efforts to bolster cybersecurity frameworks, the COVID-19 pandemic and associated digital solutions have provided a case study for challenges and opportunities related to gender-inclusive cybersecurity.

The COVID-19 pandemic underscores the critical nature of safe and reliable access to information and communication. **Internet restrictions** in Myanmar, Bangladesh and Pakistan, disproportionately impact women and girls, who are less likely to be able to access COVID-19 information through alternative means as a result of gender discrimination and social norms preventing them from speaking with others or leaving their homes to obtain information.

Telecommunication restrictions have prevented women and girls from accessing COVID-19 helplines, including helplines for gender-based violence. With a global surge in the frequency and intensity of family violence, including intimate partner violence, during COVID-19, disrupted access could have devastating results for women and girls. Perpetrators have also weaponised telecommunications, installing spyware on smartphones that allows them to stalk, track, monitor and harass women and girls in real-time.

Women at every level, from politicians, to human rights defenders, to ordinary users, face **online harassment and threats**, which in some instances has led to attacks on their physical safety. Evidence shows that since the introduction of COVID-19 lockdowns and quarantines, online misogynistic hate speech and the spread of misinformation has grown. In May, there was a 100% increase week on week[i] in tweets containing misogynistic language and references. Efforts have also been made to disrupt Twitter hashtags supporting women and girls, including #eachonereachone, started by women to raise awareness of violence against women and girls.



Digital platforms provide anonymity for perpetrators, creating an online culture of impunity. In India, a woman human rights defender was the subject of a threatening social media campaign that included fake pornographic content, while detained for protesting. Online harassment poses specific threats to women and their safety online, as well as their ability to promote a culture of peace through digital engagement.

Coinciding with an increase in working from unsecure networks at home, the use of electronic transactions for basic necessities, and mandatory online registrations for entering public spaces, has been an increase in **cybercrime**. During the current crisis, there has been a 600% increase in malicious emails, with cyberattacks on ICTs occurring every 39 seconds.[ii] Thailand has warned of fraudulent websites designed to acquire individuals' personal information that mimic the name of government platforms used to register people as they enter and leave stores and shopping centers, the majority of which are women and girls.

Additionally, lockdowns and travel restrictions have resulted in a spike in the **online sexual exploitation and abuse** of women and girls, including commercial sexual exploitation and an increase in people attempting to access illegal websites featuring child sexual abuse material. Online sexual exploitation and abuse is often accompanied by or can lead to in-person sexual and gender-based violence against women and girls.

Criminal networks and organisations are taking advantage of the sudden and prolonged increase of women and girls online. **Trafficking and migrant smuggling** networks are recruiting women and girls online that are vulnerable to negative coping mechanisms as a result of the socio-economic impacts of COVID-19. Myanmar has reported an increase in trafficking of women and girls for the purposes of forced labour, sexual servitude, and forced marriage. Online recruitment has long been a tactic of **violent extremist organisations** but grievances associated with the COVID-19 pandemic have resulted in new drivers of radicalization increasing vulnerability to recruitment.

During the COVID-19 pandemic, laws governing alleged "fake news" and online media have been used to **restrict freedom of expression** and tighten censorship. Arrests for expressing discontent or allegedly spreading false information have been reported widely across the region, including in Bangladesh, Cambodia, China, India, Malaysia, Myanmar, Nepal, the Philippines, Sri Lanka, Thailand, and Viet Nam, In the Philippines, human rights lawyer and Senator Leila de Lima was prohibited from participating in Senate sessions via teleconference. In some instances, women who have criticized responses to COVID-19 have been detained, their IP addresses removed, and their social media accounts suspended.

More and more governments across the region have adopted **digital surveillance and contact tracing** applications to stem the pandemic, including Australia, Republic of Korea, China, and many more. Like other emergency powers, the use of such applications must be proportionate, neither arbitrary nor discriminatory, respectful of human dignity, subject to review, and limited in duration. Further, the distinct consequences of digital surveillance and contact tracing for women and girls must be addressed, violations of their human rights prevented, and avenues for women human rights defenders to continue their work in the digital space protected.

STRENGTHENING CYBERSECURITY THROUGH THE WPS AGENDA

The digital world underpins every structure and system of modern life. For women and girls who rely on the digital world in the face of unequal power structures, gender-inclusive cybersecurity frameworks can provide for a digital space where the rule of law and the rights of women and girls are respected.

As with most security infrastructure, there is a significant **gender gap in cybersecurity** - in Asia and the Pacific, women account for less than 10% of the cybersecurity workforce. This gap in women's participation has resulted in a lack of gender perspectives informing cybersecurity and the development of cybersecurity frameworks that fail to identify and respond to cyberthreats faced by women and girls. This is further compounded by the low number of states that have enacted legislation to protect individuals' online data and privacy - less than 40% of states in Asia and the Pacific have legislation protecting online data and privacy.[iii]

In addition, cybersecurity is often predicated on **artificial intelligence and algorithms**, with limited civilian oversight.

With 78% of artificial intelligence professionals being men, male experiences have overwhelmingly informed algorithm creation. This has direct peace and security implications for women. For example, algorithms used in the criminal justice system overpredict the risk for women to reoffend, leading to disproportionate sentencing for women and negatively impacting their access to non-custodial settings.

Cybersecurity affects everyone - women, men, girls and boys. Advancing cybersecurity using the women, peace and security agenda can ensure a gender-inclusive cyberworld that protects the rights of women and girls, and that lessons learned from traditional peace and security processes are incorporated for the benefit of a sustainable open, free and stable digital world.

Participation: Increasing women's participation in cybersecurity and decision-making relating to the digital world is a crucial step to ensuring that the spectrum of cyber risks are addressed. Women are best placed to identify their unique cybersecurity needs, and contribute their lived experiences to the knowledge-base, informing cybersecurity, yet their representation remains low. Women's representation in the UN Group of Governmental Experts on the use of ICTs, responsible for examining existing and emerging cyberthreats, among other things, has averaged 20%[iv] since its inception, well below the recommended 30% for influence. Cybersecurity frameworks that are developed with women and reflect a gender perspective will reduce the overall risk to the cyber world.

Prevention: Incorporating a gender perspective into cybersecurity can catalyze broader peace and security efforts. Online gender-based patterns and early warning systems can highlight the emergence of conflict, as well as inform community resilience. For example, online reporting of increases in violence against women and girls can provide an early indication of potential intercommunal violence, and online hostile misogynistic messaging and behavior can indicate vulnerability to radicalization and violent extremism. Additionally, women and girls can be empowered to use their digital voices to disrupt and counter misogynistic narratives, as was the case when UN Women supported comedians in India, Indonesia, and Malaysia to counter gender stereotypes used by violent extremist organisations through online videos.

Protection: Globally, states have agreed that international law applies to cyberspace.[v] This has been reiterated at the regional level, including by ASEAN member states.[vi] Central to a cyberspace where the rule of law is respected is protecting the human rights of all users. The lack of gender perspectives in cybersecurity frameworks to date requires that particular attention and consideration be given to accelerating the protection of the human rights of women and girls. In doing so, cyberthreats that impact women and girls, such as online sexual exploitation and abuse, will be better addressed, and vulnerabilities to cybercrime and crimes facilitated through digital means, such as recruitment of women and girls by trafficking networks, reduced.

Peacebuilding: Women human rights defenders and civil society organisations have leveraged the digital world to increase the accessibility and applicability of their peacebuilding work. Women peacebuilders are using digital alert systems to quickly gather and share views on peace and security priorities with mediators and negotiators, they have developed low-tech solutions based on graphics and voice recordings to reach women and girls most vulnerable, including women and girls with disabilities, and they have provided digital literacy trainings to empower women and girls to increase their participation in public affairs and raise their digital voice. There are no limits to the peacebuilding work women can do online but the digital space for their engagement must be protected.

RECOMMENDATIONS

1. **Address gender blind spots in cybersecurity frameworks**

   With the participation of women, including civil society and women human rights defenders, assess the gender-responsiveness of existing cybersecurity frameworks, including as they relate to online data and privacy, and develop and strengthen gender-inclusive cybersecurity laws, policies and practices that respect the rights of women and girls and are able to identify and respond to their cybersecurity needs.

2. **Support the digital citizenship of women and girls for online peacebuilding**

   Support women and girls to have access to the internet and telecommunications, particularly in times of emergency, such as the COVID-19 pandemic, and in fragile and conflict settings, noting the critical nature of safe and reliable information and communications during these times. Support the digital literacy of women and girls, increasing their digital awareness and reducing their vulnerability to cyberthreats.

3. **Protect the security of women and girls in the cyberworld**

   The digital space for women and girls' civic engagement must be protected, and platforms for raising and addressing women human rights concerns supported. Cybersecurity initiatives, including digital surveillance must be fully transparent, not infringe on women and girls' rights, and contain avenues to address the misuse of data.

[i] Related to Tweets from India, Indonesia, and the Philippines from 1 May – 22 May 2020.
[ii] UNODA, Briefing by High-Representative for Disarmament Affairs, 22 May 2020.
[iii] UNCTAD Data Tracker (2020)
[iv] APC and WILFP, Why Gender Matters in International Cybersecurity, April 2020.
[v] A/RES/70/237.
[vi] ASEAN Regional Forum, 19th Session.