RESEARCH SUMMARY

CYBERSECURITY THREATS, VULNERABILITIES AND RESILIENCE AMONG WOMEN HUMAN RIGHTS DEFENDERS AND CIVIL SOCIETY IN SOUTH-EAST ASIA

UNU Macau

UN WOMEN

Background

The Women, Peace and Security (WPS) agenda recognizes that women are often excluded in security processes and encourages their leadership and meaningful participation in peace efforts across all spheres of public and private life. Women human rights defenders (WHRDs) and women's Civil Society Organisations (WCSOs) are critical for the advancement and implementation of the WPS agenda.[1]

Recognising the role of WHRDs and WCSOs in advancing inclusive and sustainable peace, and their increasing dependency on digital tools and platforms to conduct their work, this research examined the cybersecurity posture of these groups in South-East Asia, the risks they face with rapid digital transformation, and the implications for peace and conflict-prevention efforts.

The Research

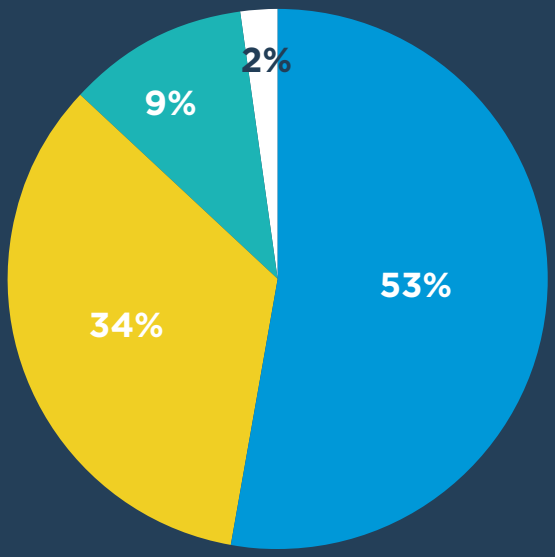
While there is increasing awareness of the risks women and girls face in cyberspace, there is little understanding of the impacts of gender on cybersecurity – or the processes and practices used to protect digital systems and networks from cyber risks and their harms. Also, there have few evidence-based efforts investigating WCSOs and WHRDS experiences of cybersecurity threats, their cyber vulnerabilities, and the ways they enact cyber resilience.

In this research, UN Women and the United Nations University Institute in Macau take a gendered lens and human-centric approach to understanding cybersecurity in South-East Asia, acknowledging that women are disproportionally negatively affected by cybersecurity risks and that WHRDs and WCSOs are often specifically targeted especially in politically volatile and conflict- and crisis-affected contexts and situations where civic space is shrinking. This work differs from previous research in three critical ways as shown in the table (1), on page 3.

1 The United Nations Secretary General's Annual Report on Women, Peace and Security from 2022, among others, stresses the importance of the work of WHRDs, stating that "the unconditional defence of women's rights is one of the most visible markers of the work of the United Nations on peace and security" (S/2022/272).

SURVEY DEMOGRAPHICS

Individual level



Organisation level

69% directly served women and girls

38% women and girls were the primary target group of their organization

The majority of participants (n = 55; 69 per cent) indicated that they directly served women and girls, and 30 (38 per cent) indicated that women and girls were the primary target group of their organization. To categorize organizations as WCSOs as compared to general CSOs, the main aims of each entry were checked alongside information about clientele.

This resulted in 56 (70 per cent) of the participants being categorized as working for a WCSO and 24 working for general CSOs.

56 working for CSOs

24 working for CSOs

For the purposes of the analyses, in most instances, overall statistics are provided, but in some instances, group comparisons are made to illustrate differences and similarities by:

Gender:
women and gender diverse persons (n = 51) as compared to men (n = 27), and

Type of organization:
WCSO (n = 56) and CSO (n = 24).

Interview demographics

The sample comprised 20 women and one man from a diverse range of international, national and regional organizations.

COUNTRY	SURVEY SAMPLE	INTERVIEW SAMPLE
Cambodia	19	3
Lao PDR	6	-
Myanmar	8	-
Thailand	12	10
Viet Nam	7	-
Regional	-	1
Total	80	21

TABLE 1.

A focus on human-centric as compared to techno-centric cybersecurity	The goal of techno-centric cybersecurity is to prevent adverse events secure technical assets (i.e., infrastructure, systems, software and platforms) and the information contained therein. Human-centric cybersecurity positions reorients thinking toward human safety as the main aim of cybersecurity processes, practices, and regulations.
An emphasis of human factors rather than technical skills in cybersecurity	Although digital skills are critical to achieving cybersecurity, psychological and behavioural factors have a major influence of information and systems security practices. We highlight that people (their motivations, feelings, and experiences) play an important role in perpetrating, preventing, responding, and recovering from cyber risks.
Centralisation of gender as critical to cybersecurity	Online gender dynamics perpetuate existing power relationships and inequalities that are prevalent offline such that women tend to experience greater online violence. There are also gendered differences in access to and uses of digital technologies, behaviour, and interactions online – these all affect cybersecurity and cyber resilience.

The aim of the research was to generate knowledge on ***cybersecurity risks and vulnerabilities faced by WCSOs and WHRDs with a goal of promoting cyber resilience and the human and digital rights of women in all their diversity across South-East Asia.*** To achieve this aim, the research undertook mixed-methods approach including a review of the literature and national indicators, surveys with WCSOs, and interviews with WHRDs in the South-East Asia region.

Key Findings

WHRDs and WCSOs rely on digital technologies for their work

Technology has the potential to support WCSOs and WHRDs in facilitating and leveraging their work. Digital technologies, especially social media, are used to connect with beneficiaries and partners, raise awareness about women's rights issues, and mobilise support for their work. WCSOs and WHRDs are increasingly reliant on personal devices for their work. This has given rise to increased cybersecurity risks because these devices are not always secure, and organisations often lack strong formal data protection policies and procedures. Encrypted messaging applications are seen as a critical feature for ensuring the confidentiality of communications for WCSOs and WHRDs.

- 89% of WCSOs consider technology as very important for their work
- Technologies were described as "like our life, the life of the work", enabling to connect, call to action, and support day-to-day work
- Personal devices (laptops and mobile phones) are often used due to lack of access to work devices and this often increases security risks
- Social media is a critical tool for operations, but raises challenges for cybersecurity risk exposure

The Cyber Threat Landscape for WCSOs and WHRDs differs from other actors

WCSOs and WHRDs in South-East Asia are at high risk of experiencing a range of cyber threats. They are largely aware of these risks but not necessarily able or ready to prepare for them or to actively recover from a cyber-attack. WCSOs had higher threat perceptions and threat experiences compared to non-women led CSOs - the largest differences being for online harassment, trolling, and doxxing (see Figures 1 and 2). Notably, there was a high prevalence of both experiences and

perceptions of threat across all of the indicators. Cyber-bombing and impersonation of organisations on social media were also found to be important, emerging threats. Furthermore, cyber threats were understood to be gendered in nature, whereby WCSOs and WHRDs were specifically targeted due to the focus of their work and were likely to be attacked with misogynistic and sexualised harassment.

Cyber Vulnerabilities of WCSOs and WHRDs

Participants had high levels of digital self-efficacy and engaged in good information security practices in general. But there are important areas where individuals were less secure and confident online, such as managing their digital footprint and solving technical issues. Key vulnerabilities were the lack of device protection (especially for personal devices), the use of unlicensed software, and insufficient organizational policies and procedures. The most common insecure practices among WCSOs were posting about work on social media and downloading potentially risky files to complete work (see Figures 3 and 4).

Recommendations

The results of the research highlight that digital technologies have a central function for WCSOs and WHRDs in their work and are now critical tools used to engage in advocacy and activism. However, this new reliance on technology can also expose individuals and organisations to cyber threats that may disrupt their work, damage their reputation, and even create harm or injury, all of which can further marginalise women's voices and participation in society and change-making processes. Three key recommendations are made on this basis of this research.

Recommendation 1.

Increase knowledge and awareness of gendered cybersecurity threats and vulnerabilities among civil society, governments, private-sector actors and other decision makers.

- Engage in awareness raising campaigns to highlight the prevalence and impacts of cyberattacks on women's civic engagement and peace efforts. A focus of human-centric cybersecurity, the protection of human rights, and the minimisation of harms should be taken.
- Document stories and lived experiences of WCSOs and WHRS and their experiences related to gendered cybersecurity threats and vulnerabilities
- Conduct additional research on cybersecurity that is contextualised to the sociocultural context and specific conditions of diverse groups of women and disseminate the findings in policy relevant, accessible ways. This includes conducting more targeted research focusing on conflict- and crisis affected areas, recognising the unique cybersecurity challenges these contexts bring about.

Recommendation 2.

Foster inclusive and collaborative approaches in cybersecurity policy development and engagement

- Advance multi-sectoral and multi-stakeholder dialogue on cybersecurity-related laws, policies and practices, fostering a culture of collaboration and multilateralism. These dialogues should take a whole-of-society approach, ensuring equal engagement from civil society, governments, academics and private-sector actors. This should be done with an inclusive approach in which WCSOs and WHRDs are part of the design process — not merely consulted when the agenda has already been set.
- Provide targeted support to WCSOs and WHRDs to lead and participate in negotiations and decision-making processes relating to cybersecurity-related laws and policies at all levels, for example, by supporting their participation in local, national, regional and global policy-making processes (including in cyber diplomacy forums) as well as in deliberations with private companies.
- Base the development and implementation of cybersecurity-related laws, policies and practices on international best practices and clauses outlined in international law , human rights conventions and WPS commitments.
- Conduct intersectional human rights impact assessments as part of cybersecurity-related law and policy development processes, including looking at factors such as gender, age, ability and other backgrounds. This applies to both government and private-sector actors.

FIGURE 1. WCSOs' EXPERIENCES OF CYBER THREATS

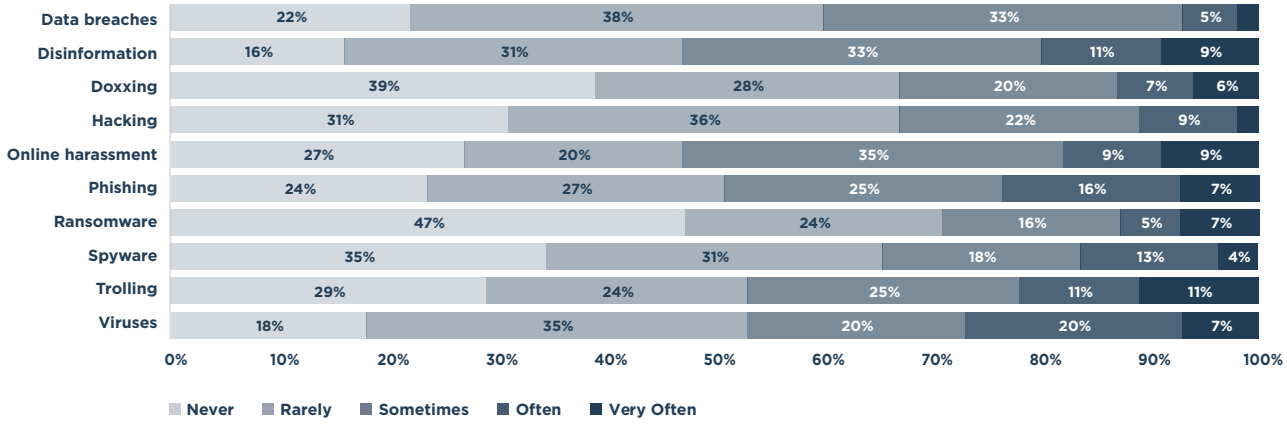


FIGURE 2. NON-WOMEN-LED CSOs' EXPERIENCES OF CYBER THREATS

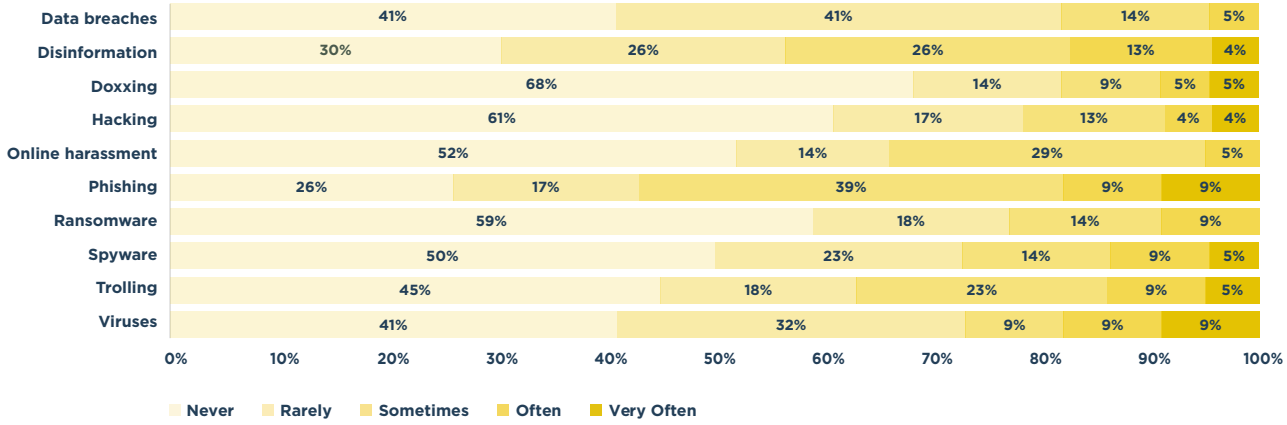


FIGURE 3. WCSOs INFORMATION SECURITY BEHAVIOURS

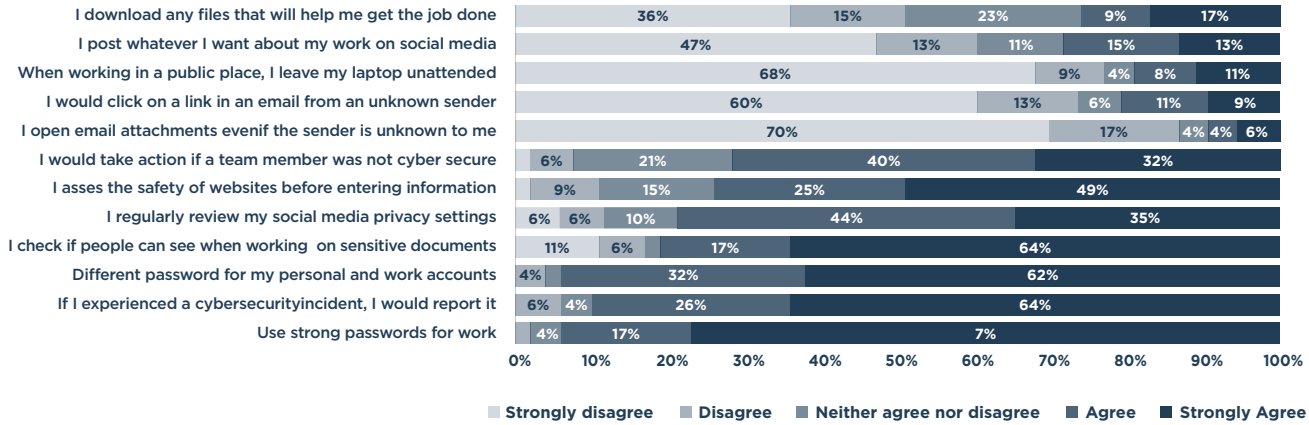
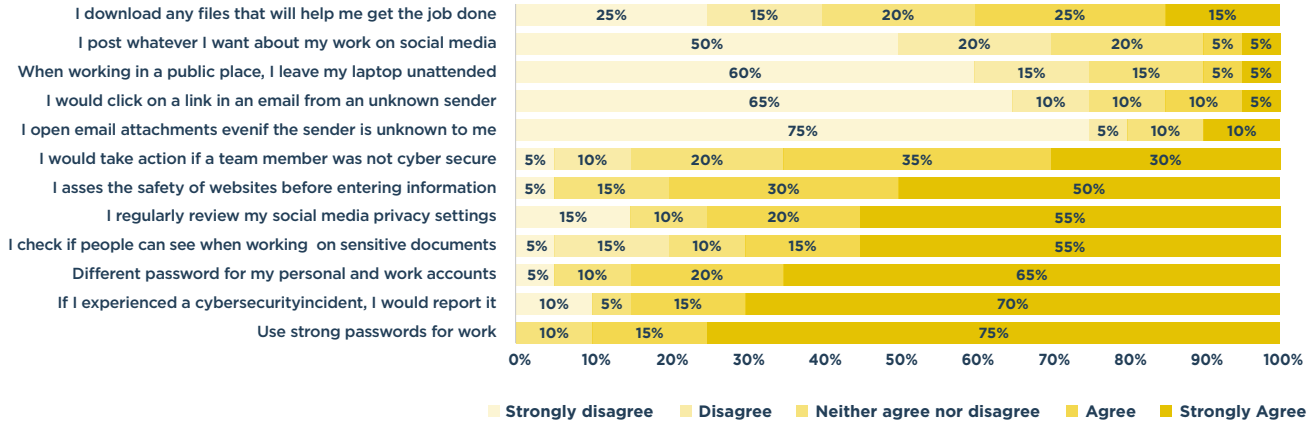


FIGURE 4. CSOs INFORMATION SECURITY BEHAVIOURS



Recommendation 3.

Build knowledge and strengthen capacities of civil society, government, private-sector actors and other decision makers to develop appropriate means of prevention and response to cyberattacks and their disproportionate impacts on WCSOs and WHRDs.

- Based on evidence collected (see recommendation 1), co-create contextualized resources (e.g., guidelines, toolkits, repositories) to prevent, respond to and recover from cyber threats and mitigate cyber vulnerabilities. Target technical support and capacity building to the specific areas of identified needs, gaps and vulnerabilities of WCSOs and WHRDS. Context-specific needs should be identified through intersectional and gender-responsive assessments in close dialogue with WCSOs and WHRDs.
- Dedicate resources and deliver targeted, accessible, and inclusive capacity building activities for WCSOs and WHRDs concerning cybersecurity and support community-based training and empowerment activities. Specific attention should be given to individuals and organizations particularly at risk, such as WCSOs and WHRDs operating in politically volatile and conflict- and crisis-affected contexts and situations where civic space is shrinking.
- Provide needs-based, inclusive, and gender-responsive cybersecurity support to WCSOs and WHRDs, including technical support, software, funding and other resources for preventive, emergency response and recovery purposes. This can, for instance, include in-person training and readily available e-learning materials.
- Create platforms and mechanisms to monitor, report, and collect data on cyberattacks targeting WCSOs and WHRDs, in a manner that is mindful of their privacy, in order to facilitate a better overview of the scope of the issue.

This brief summarises the report **'Cybersecurity Threats, Vulnerabilities and Resilience among Women Human Rights Defenders and Civil Society in South-East Asia'** written by Jaimee Stuart, Senior Researcher -Team Lead, UNU, with contributions from Cara Antonaccio and Min Yang and in collaboration with Mamello Thinyane, Kris Villnueva-Libunao and Arthit Suriyawongkul. Further technical input and support was provided by Gaëlle Demolis and Alexandra Håkansson Schmidt from UN Women. (https://doi.org/10.17605/OSF.IO/H38WZ)

Thank you to the Government of Australia, under the Cyber and Critical Tech Cooperation Program of the Department of Foreign Affairs and Trade, and to the Government of the Republic of Korea for their support of this research and of the UN Women project entitled Women, Peace and Cybersecurity: Promoting Women's Peace and Security in the Digital World.

May 2024

Ministry of Gender Equality and Family

Australian Government

CYBER & CRITICAL TECH COOPERATION PROGRAM