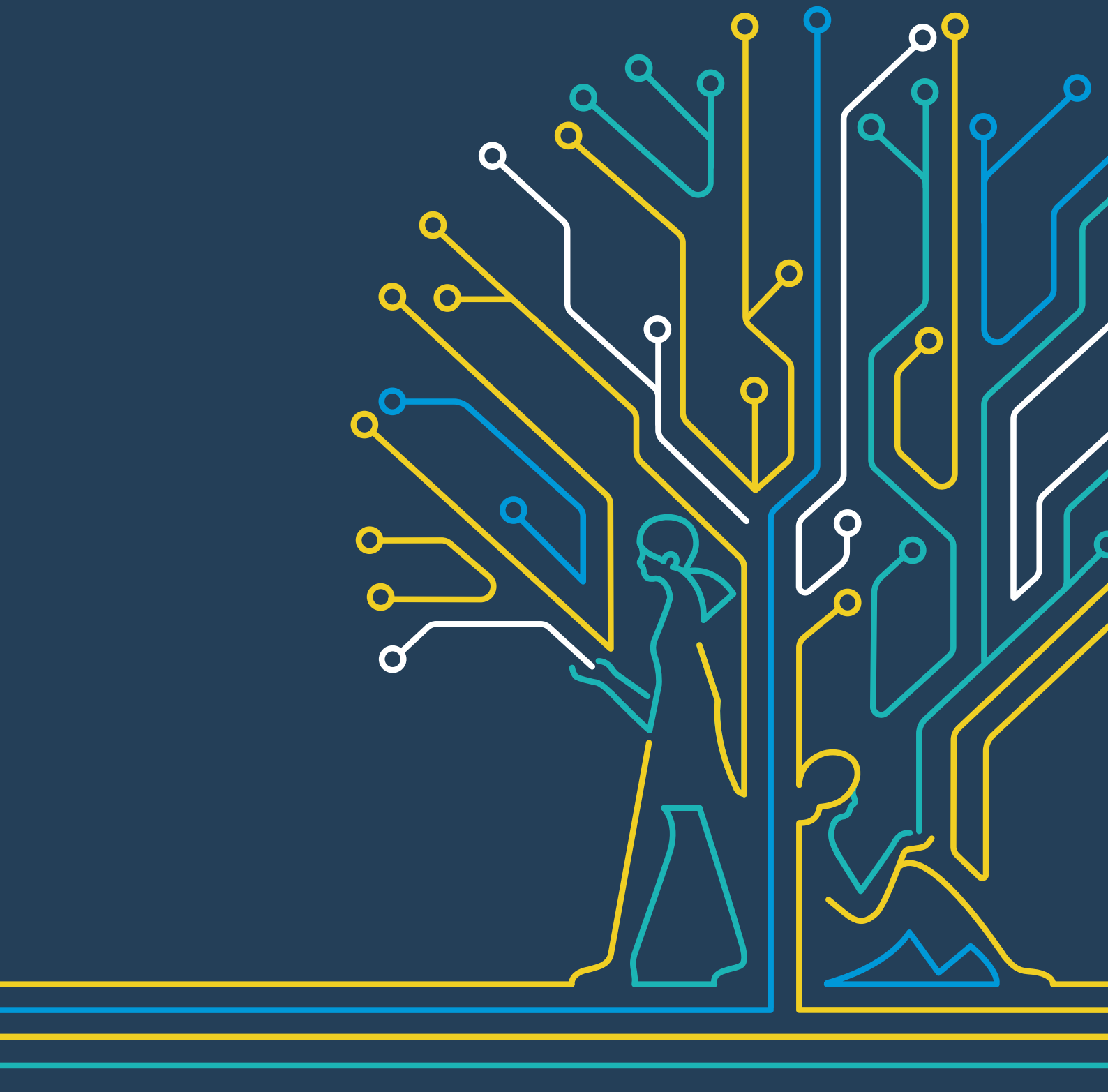
UNU Macau

UN WOMEN

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



ACKNOWLEDGEMENTS

This research was undertaken as part of the UN Women Regional Office for Asia and the Pacific project, Women, Peace and Cybersecurity: Promoting Women's Peace and Security in the Digital World, with the generous support of the Government of Australia, under the Cyber and Critical Tech Cooperation Program (CCTCP), and of the Government of the Republic of Korea.

Exploring the connections between the Women, Peace and Security Agenda and cybersecurity is a key component 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 (2023-2027).

This report was written by Jaimee Stuart, Senior Researcher -Team Lead, UN University Institute in Macau (UNU Macau), with contributions from Cara Antonaccio and Min Yang, and in collaboration with Mamello Thinyane, Kris Villnueva-Libunao and Arthit Suriyawongkul. Additionally, the team benefited from valuable technical input and support from Gaëlle Demolis and Alexandra Håkansson Schmidt from the UN Women Regional Office for Asia and the Pacific.

Published by the UN Women Regional Office for Asia and the Pacific.
https://doi.org/10.17605/OSF.IO/H38WZ

UNU Macau

UN WOMEN

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

Ministry of Gender Equality and Family

Australian Government

CYBER & CRITICAL TECH COOPERATION PROGRAM

TABLE OF CONTENTS

GLOSSARY

Cyber assets / Cyber resources	The technologies and the affordances they provide to enable personal or organizational functionality, produce value and achieve goals. These include tangible (physical) and intangible (nonphysical) assets.
Cyberattack	A type of cyber threat involving a malicious act against a person, organization or nation, violating its security and intentionally causing damage. It typically includes deliberate acts to harm or exploit digital systems, information or processes.
Cyber threats	Adverse cyber incidents that have the potential to cause harm to individuals, organizations and entities through technological systems and the way they are used, e.g. by compromising the functional capacity of assets, exploiting cyber vulnerabilities, or by leveraging social and psychological vulnerabilities.
Cyber vulnerabilities	Weaknesses, both technical or non-technical, that can exacerbate the harms caused by or the likelihood of exploitation and exposure to cyber threats.
Cyber resilience	The state of, or dynamic process in which, an individual, organization or entity can effectively maintain continuity or enhance operations through the prevention, disruption and mitigation of cyber threats with the result of minimizing harm.
Cyber-bombing / Zoom-bombing	A type of cyberattack in which an individual or a group of unwanted and uninvited users interrupt online meetings and events for the purpose of disruption.
Cybersecurity	A state in which information and/or computer systems and networks are free from threat as well as the set of practices undertaken by individuals and organizations to ensure such security.
Data breach	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.
Distributed denial of service (DDOS)	A type of cyberattack where threat actors make digital resources unavailable to or unusable by legitimate users by disrupting or flooding the services of a host connected to a network.
Doxxing	Private or identifying information distributed about a person on the Internet with deliberate negative intent.
Encryption	The process of encoding information to prevent anyone other than its intended recipient from viewing it.

Hacking	Unauthorized access to or control over computer network security systems for an illicit purpose.
Human-centric cybersecurity	Centralizing people (rather than technology) as the primary subjects of cybersecurity practice.
Malware	Any program or file that is intentionally harmful (i.e. malicious) to a computer, network or server.
Misinformation	Incorrect or misleading information, which, in contrast to disinformation, is not spread to knowingly deceive its recipient.
Multi-factor authentication (MFA)	A multi-step account login process that requires users to enter more information than just a password.
Phishing	Malicious emails designed to trick people into falling for a scam, divulging sensitive information or taking other action against their or their organization's interests.
Ransomware	A type of malware that is designed to block access to a computer system until a sum of money is paid.
Spyware	A type of malware that is designed to enter a device, gather data and forward it to a third party without consent.
Trolling	Deliberate attempts to offend, inflame, attack or provoke.
Virtual private network (VPN)	A mechanism for creating a secure connection between a device and a network.
Virus	A type of malware that, when executed, can self-replicate, infect / modify other programs and spread to other computers.

LIST OF FIGURES

LIST OF TABLES

1.

EXECUTIVE SUMMARY

The Women, Peace and Security (WPS) agenda broadly addresses the disproportionate impacts of conflict on women and girls, highlights that women are often excluded in security processes and encourages their leadership and meaningful participation in making lasting change in international and national peace efforts. As digital transformation has altered all aspects of daily life and expanded the places and spaces where we interact, the WPS agenda is increasingly applied to emerging digital security issues. However, despite the growing importance of cyberspace to national and international security, the United Nations Security Council Resolutions (UNSCR) that constitute the WPS agenda have yet to explicitly mention cybersecurity. This research, therefore, is situated at the nexus of the WPS agenda and cybersecurity.

Women human rights defenders (WHRDs) and women's grass-roots organizations are at the forefront of the development, advancement and implementation of the WPS agenda. As outlined in the United Nations Secretary General's Annual Report on Women, Peace and Security from 2022, "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," to which the work of WHRDs is paramount.[1] By recognizing the indispensable role that WHRDs and women's civil society organizations (WCSOs) have in advancing inclusive and sustainable peace, this research will contribute to a better understanding of the cybersecurity posture of these groups in Southeast Asia, the risks they face in the slipstream of rapid digitization, and the overall implications of their actions for peace and conflict-prevention efforts.

Cybersecurity comprises a collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect resources (in the many ways that these are conceptualized). Gendered dynamics are prevalent in cybersecurity for many reasons: women and men experience cyber risks differently, there are gendered disparities in the degree of participation in the formation and enactment of cybersecurity policies and practices, and the cybersecurity field is marred by masculinized gender norms.[2, 3, 4] Civil society actors and human rights defenders who advocate on behalf of women and girls experience a range of heightened threats and vulnerabilities in cyberspace.[5] These issues are compounded by the social, political and cultural contexts that shape the experiences of women and girls in Southeast Asia, who face a greater likelihood of online and offline gender-based discrimination and violence.[6]

1 United Nations Security Council (2022). *Women, Peace and Security – Report of the Secretary General*, S/2022/740, 1.
2 Brown, D., & Pytlak, A. (2020). *Why Gender Matters in International Cyber Security*. www.wilpf.org
3 Millar, K., Shires, J., & Tropina, T. (2021). *Gender Approaches to Cybersecurity: Design, Defence and Response*. https://doi.org/10.37559/GEN/21/01
4 Strohmayer, A., Bellini, R., & Slupska, J. (2022). Safety as a Grand Challenge in Pervasive Computing: Using Feminist Epistemologies to Shift the Paradigm From Security to Safety. *IEEE Pervasive Computing, 21*(3), 61–69. https://doi.org/10.1109/MPRV.2022.3182222
5 Lewis, R., Rowe, M., & Wiper, C. (2017). Online abuse of feminists as an emerging form of violence against women and girls. *British Journal of Criminology, 57*(6), 1462–1481. https://doi.org/10.1093/bjc/azw073
6 Timur, F. B. (2022). Asean and Gendered Violence in Cyberspace. *Gender and Security in Digital Space*, 51–68. https://doi.org/10.4324/9781003261605-6

While there is some awareness of the risks women and girls face in cyberspace, there is little evidence concerning the prevalent threats and vulnerabilities that organizations and individuals who advocate on behalf of women and girls face. Nor has there been any significant research that seeks to understand how WCSOs and WHRDS manage cybersecurity threats and vulnerabilities (i.e. the processes of cyber resilience). To address these challenges, this research considers the cybersecurity landscape of Southeast Asia and the unique (and potentially risky) position of WCSOs and WHRDs; frames cybersecurity from a gendered perspective in terms of the individual, social and environmental factors that may increase or perpetuate cyber threats and vulnerabilities; and focuses on cyber resilience as a critical mechanism for mitigating the potential harms that may result from risks to cybersecurity. This research aims **to generate knowledge to reduce cybersecurity risks and increase cyber resilience with a goal of promoting the human and digital rights of women in all their diversity in Southeast Asia**.

To achieve these aims, the research undertook a mixed-methods approach, including a review of secondary sources and the collection of primary data through surveys and interviews, both with a specific focus on the Southeast Asia region. Key findings of the research include:

1. THE IMPORTANCE OF DIGITAL TECHNOLOGIES

Research results underscore that digital technologies are essential for WCSOs and WHRDs to effectively carry out their work. Individuals and organizations use digital technologies to mobilize support, raise awareness about women's rights issues and to work and connect with their beneficiaries, partners and stakeholders. Research results also suggest that WCSOs and WHRDs are increasingly reliant on personal devices for their work, which is a cybersecurity concern because these devices are not always secure. Furthermore, organizations often lack strong formal data protection policies and procedures that are sensitive to the blurred lines of personal and professional digital assets.

2. THE RISKS AND BENEFITS OF SOCIAL MEDIA

Social media was found to be a powerful tool that organizations and activists use to raise awareness drive social change, engage in external communications and outreach, gather volunteers and to privately and safely connect with individuals and groups. WCSOs and WHRDs particularly saw encrypted messaging applications as a critical tool for ensuring the confidentiality of communications. Some important challenges were raised with safely using social media, including data compromise and misuse, the overlap between personal and professional social media communications, and increased exposure to cyberattacks and threats.

3. THE CYBER THREAT LANDSCAPE FOR WCSOs AND WHRDs

Research findings broadly indicate that WCSOs and WHRDs in Southeast Asia are at high risk of experiencing a range of cyber threats and further that they are largely aware of these risks but are not necessarily able or ready to prepare for them or to actively recover from a cyberattack.

The most commonly reported cyber threats were disinformation, online harassment, phishing and trolling. The most impactful threats were perceived to be data breaches, spyware and viruses. Notably, there was a high prevalence of both experiences and perceptions of threat across all indicators. 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 sexualized harassment.

4. DIGITAL SELF-EFFICACY AS A CRITICAL CYBERSECURITY LEVER

With respect to cybersecurity behaviours and beliefs, findings indicate that although some participants have high levels of digital self-efficacy, there are important areas where participants felt less confident in their ability to safely use digital technologies, such as managing their digital footprint or solving technical issues. In addition, a strong association was found between digital self-efficacy and information security practices, which suggests that efforts to increase digital self-efficacy could be an important way to improve cybersecurity behaviours and strengthen organizational cyber resilience. In addition, while participants felt most confident in their organization's ability to prepare for cyber threats, by comparison, they felt less confident in their organization's ability to recover from cyber threats. This suggests that beyond encouraging preventive and precautionary approaches, more work is needed to cultivate cyber resilience in an increasingly complex context of threats, and, in particular, recognizing and responding to the gendered dynamics as well as eventual political and conflict-related challenges of these.

1.1 Conclusion and Recommendations

The research findings point to key gender differences in cyber threats and vulnerabilities, including that women are disproportionately targeted by cyber threats that are motivated by negative stereotypes and misogynism, as well as by the political nature of the work that women's organizations and activists engage in. Findings indicate that these cyber threats can have major impacts on the health and well-being of those affected and can lead to their withdraw from advocacy and activism. Moreover, supporting existing evidence the research highlighted a lack of effective and rights-based laws and policies in place to protect WCSOs and WHRDs online, which further exacerbated the negative effects of cyber threats and attacks. Overall, findings suggest that gender is an important factor shaping who is targeted by cyber threats and that cyber threats have an important impact on the work of WCSOs and WHRDs, and hence also to the advancement of the WPS agenda and compliance with related commitments.

The research results shed light on the importance of digital technologies for WCSOs and WHRDs, as well as the cross-cutting effects of cyber threats and vulnerabilities in this context. Cybersecurity is a serious concern for WCSOs and WHRDs; the lack of appropriate and relevant mechanisms to protect and prevent cyber harms can further marginalize women's voices and participation in decision making, peace processes and in society in general. Ultimately, the research findings indicate a need for greater awareness of the gender dimensions of cybersecurity in Southeast Asia, as well as for more effective measures to enhance cyber resilience among WCSOs and WHRDs.

Critically, the research findings indicate there is a need for a strong shift away from techno-centric and generic approaches to human-centred and contextualized approaches to cyber resilience that centralize gender. This is a key to holistically safeguarding the work and commitments of WCSOs and WHRDs, particularly in politically volatile and conflict- and crisis-affected contexts. Ultimately, this will also have implications for the implementation of the WPS agenda, as such measures are needed to ensure that said groups can uphold their leadership and participation in peace efforts, conflict prevention and decision-making processes and that they have access to appropriate protection and relief and recovery services. As such, this report suggests two overarching recommendations (outlined in more detail in Section 5.1, Key Recommendations).

- **Recommendation 1.**
  Increase knowledge and awareness of gendered cybersecurity threats and vulnerabilities among civil society, governments, private private-sector actors, and other decision-makers.

- **Recommendation 2.**
  Foster inclusive and collaborative approaches in cybersecurity policy development and engagement.

- **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.

2.

BACKGROUND

The framing of this research requires a nuanced conceptualization of the issues being investigated (i.e. cybersecurity) and an understanding of risks (i.e. cyber threats and vulnerabilities and their interactions) as well as the management of impacts and outcomes (i.e. cyber resilience and harms). While these concepts have been researched in other domains (e.g. governments and the private sector), there is limited research from a gendered perspective for civil society and minimal research that draws these issues together in the Southeast Asian context. The following section outlines the core constructs under investigation as aligned with the goals of the WPS agenda: promoting women's leadership, empowerment, peace, and security as associated with the uses and affordances of digital technologies and the experiences of women and girls within digital environments.

2.1 Human-Centric Cybersecurity

Cybersecurity is broadly defined as both a state in which information and/or computer systems and networks are free from threat as well as the set of practices undertaken by individuals and organizations to ensure such security. This definition focuses on digital devices and systems as the target of protection as highlighted by the International Telecommunication Union:

"the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."[7]

For this research, the traditional framing of cybersecurity is limiting for several reasons. First, a techno-centric focus neglects the human and social aspects of cybersecurity. Second, too much of a focus on the prevention of known threats risks overlooking new risks. Third, organizations are composed of individuals who interact and engage with each other in ways that influence and impact cybersecurity, meaning that organizational cyber risks are not separate from individual behaviours. Finally, only addressing cybersecurity as a national security concern gives little room for discussing human rights and may even harm or overshadow individual rights in the pursuit of security.[8] To address these limitations, this project adopts a human-centric perspective on cybersecurity and emphasizes the importance of taking a gendered lens to cyber risks and outcomes.[9,10]

A human-centric cybersecurity approach positions people (rather than technology) as the primary subject of cybersecurity, which reorients thinking towards human safety

7 International Telecommunications Union (ITU). (2008). ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: Overview of cybersecurity. https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

8 Brantly, A. F. (2014). The Cyber Losers. *Democracy and Security, 10*(2), 132–155. https://doi.org/10.1080/17419166.2014.890520

9 Brown, D., & Pytlak, A. (2020). *Why Gender Matters in International Cyber Security*. www.wilpf.org

10 Liaropoulos, A. (2015). Cyber-Security: A Human-Centric Approach. In N. Abouzakhar (Ed.), 14th European Conference on Cyber Warfare & Security (Issues 2-3 July). https://doi.org/10.13140/RG.2.1.4855.8160

as the main aim of cybersecurity processes, practices and regulations.[11] The goal of human-centred cybersecurity is to protect systems and networks so that they can support and create a foundation for the expression and exercise of human rights. These rights include access to information, freedom of thought, and freedom of association.[12] This research highlights that the protection of computers, networks and information that are central to cybersecurity should be treated as a mechanism with which to achieve human security and protect human rights.[13] Such a focus enables us to centralize concepts of safety and well-being and investigate how cybersecurity practices can threaten and/or disempower technology — and they can be used to protect and empower.

2.1.1 A GENDERED LENS ON HUMAN-CENTRED CYBERSECURITY

Gender shapes and influences access to and uses of digital technologies, behaviours, and online interactions and is a critical factor in exposure to cyber risks. Online gender dynamics often perpetuate existing power relationships and inequalities that are prevalent offline, sometimes reinforcing or even amplifying social and political structures.[14] For example, women and girls are disproportionately targeted by hate speech, online gender-based violence (e.g. sexualized online abuse), and certain cybercrimes. Issues such as non-consensual distribution of images sexual exploitation, grooming, harassment and privacy violations are common, and have been systematically deployed to discredit and silence women, particularly those in public positions such as politicians, journalists and human rights defenders. In addition, offline violence against women has strong associations with online gender-based violence, where perpetrators (individuals, organizations and other actors) use technology to directly target, surveil, stalk or harass their targets.[15]

Given the gendered nature of online risks, it is crucial to consider how these impact WCSOs and WHRDs. Notably, being able to communicate, access and share information quickly and easily is central to the work of activists and CSOs. However, those who advocate for women may be particularly susceptible to cyber threats due to the sensitive nature of their work. These groups often deal with confidential information, including the personal data of vulnerable individuals, which makes them attractive targets for cybercriminals and other adversaries. This particularly applies to human rights defenders. In addition, civil society organizations often lack the resources and technical expertise to adequately protect themselves from cyberattacks or to prepare staff to protect and empower themselves.

Moreover, advocates may be targeted with online harassment and stalking that is specifically gendered in nature, including threats of sexual violence or attempts to discredit their work by attacking their gender identity or sexuality. This can impede their activism and limit their ability to effectively engage both on- and offline, with some choosing to withdraw from such work out of fear for their or others' safety. Of critical importance, WCSOs and WHRDS may be more likely to be targeted by those who seek to silence or discredit feminist movements, challenge gender equality or suppress human rights.

2.1.2 WCSOS AND WHRDS CYBERSECURITY ISSUES IN SOUTHEAST ASIA

WCSOs and WHRDs in Southeast Asia are facing a growing range of cybersecurity risks. It has been found that those who advocate for women and girls are increasingly targeted with online harassment and abuse, including threats of violence, doxxing and hate speech.[16,17] Evidence also indicates that threat actors in Southeast Asia use surveillance technologies to monitor the online activities of civil society leaders and human rights defenders.[18, 19, 20] Merely knowing that they are under surveillance can intimidate and silence those who work with women and girls; individuals whose communications are being monitored may self-censor and be less likely to speak out about sensitive issues or engage in advocacy work. Furthermore, information gathered could be used against them — even otherwise innocuous information that is taken out of context. Such harassment substan-

11 Strohmayer, A., Bellini, R., & Slupska, J. (2022). Safety as a Grand Challenge in Pervasive Computing: Using Feminist Epistemologies to Shift the Paradigm From Security to Safety. *IEEE Pervasive Computing*, *21*(3), 61–69. https://ieeexplore.ieee.org/document/9830605

12 Deibert, R. J. (2018). Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs*, *32*(4), 411–424. https://doi.org/10.1017/S0892679418000618

13 Comninos, A., & Seneque, G. (2014). Cyber security, civil society and vulnerability in an age of communications surveillance. Global Information Society Watch, 32–40.

14 Brown, D., & Pytlak, A. (2020). *Why Gender Matters in International Cyber Security*. www.wilpf.org

15 Strohmayer, A., Bellini, R., & Slupska, J. (2022). Safety as a Grand Challenge in Pervasive Computing: Using Feminist Epistemologies to Shift the Paradigm From Security to Safety. *IEEE Pervasive Computing*, *21*(3), 61–69. https://doi.org/10.1109/MPRV.2022.3182222

16 https://www.scmp.com/news/asia/southeast-asia/article/3139104/thai-royalists-dox-hundreds-pro-democracy-activists-using

17 https://asiapacific.unwomen.org/sites/default/files/Field%20Office%20ESEAsia/Docs/Publications/2021/04/ap-WPP_online-hate-speech_brief.pdf

18 https://advox.globalvoices.org/2023/04/24/underscoring-the-challenges-of-promoting-digital-rights-in-southeast-asia/

19 https://www.devex.com/news/digital-rights-activists-in-southeast-asia-increasingly-at-risk-103946

20 https://www.reuters.com/article/china-southeast-asia-surveillance/feature-activists-fear-rising-surveillance-from-asias-digital-silk-road-idUSL8N1WDoDP

tially reduces the ability of advocates to speak out on critical human rights issues.[21,22] In this way, surveillance is a tool to suppress freedom of expression and can make it more difficult for WCSOs and WHRDs to raise awareness of important issues.[23]

Censorship of Internet content in Southeast Asia also has negative impacts on the work of WCSOs and WHRDs. Effects include reduced access to information, limited ability to communicate and increased risk of retaliation.[24, 25]

In addition to these threats and challenges, WCSOs and WHRDs in Southeast Asia also face many other barriers to safely conducting their work online, including lack of access to affordable digital technology and Internet connectivity, lack of funding for security software and licenses, lack of legal protection, misogyny and restrictive patriarchal operating contexts, and social stigma.[26, 27, 28]

2.2 Research Approach

This research takes a gendered lens and human-centric approach to understanding cybersecurity in Southeast Asia, acknowledging that women are disproportionally negatively affected by cyber risks and are under-represented in technical and decision-making roles concerning cybersecurity. Furthermore, organizations and individuals who advocate on behalf of or engage in activism related to issues of women and girls may be specifically targeted by threat actors due to the nature and content of their work.

Table 1 summarizes the research approach by outlining how it differs from previous cybersecurity research in four ways:

1. Cybersecurity has largely been framed from the state, government, and business stakeholders' perspective, often overlooking civil society stakeholders.[29, 30, 31] Therefore, this research approach focuses on the experience of WCSOs and WHRDs;
2. Research has typically been techno-centric with a focus on the confidentiality, integrity and availability goals for information and communication infrastructure and systems,[32] whereas this research is human-centric;
3. Cybersecurity as a domain has embedded gender biases (e.g. in skills development and leadership roles) that perpetuate the marginalization and vulnerability of women. Therefore, this research uses a gendered lens; and
4. Cybersecurity has traditionally focused on the prevention of cyberattacks (deliberate acts to harm or exploit digital systems, information or processes). Therefore, this research focuses on holistic understandings of cyber risks and how to mitigate the potential negative outcomes of these (i.e. cyber resilience).

21 https://ohchr.org/sites/default/files/Documents/Issues/Women/WRGS/SexualHealth/INFO_WHRD_WEB.pdf
22 https://www.ohchr.org/en/statements/2018/06/impact-online-violence-women-human-rights-defenders-and-womens-organisations
23 https://freedomhouse.org/programs/asia-pacific
24 https://thediplomat.com/2018/01/the-rapid-rise-of-censorship-in-southeast-asia/
25 https://www.chathamhouse.org/events/all/research-event/disinformation-and-censorship-freedom-expression-online-southeast-asia
26 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWxPuf
27 https://www.business-humanrights.org/en/latest-news/myanmar-asia-internet-coalition-joins-civil-society-in-raising-alarm-over-cybersecurity-law/
28 https://www.asiaglobalonline.hku.hk/leave-no-one-behind-how-include-civil-society-cybersecurity-debate
29 Comninos, A. & Seneque, G. (2014). Cyber Security, Civil Society, and Vulnerability in an Age of Communications Surveillance, GIS https://giswatch.org/en/communications-surveillance/cyber-security-civil-society-and-vulnerability-age-communications-sur
30 Liaropoulos, A. (2015). Cyber-Security: A Human-Centric Approach. In N. Abouzakhar (Ed.), *14th European Conference on Cyber Warfare & Security* (Issues 2-3 July). https://doi.org/10.13140/RG.2.1.4855.8160
31 Maschmeyer, L., Deibert, R. J., & Lindsay, J. R. (2021). A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. Journal of Information Technology and Politics, 18(1), 1–20. https://doi.org/10.1080/19331681.2020.1776658
32 Gioe, D. V., Goodman, M. S., & Wanless, A. (2019). Rebalancing cybersecurity imperatives: patching the social layer. Journal of Cyber Policy, 4(1), 117–137. https://doi.org/10.1080/23738871.2019.1604780

TABLE 1. RESEARCH APPROACH

FOCUS OF PREVIOUS RESEARCH	APPROACHES UNDERTAKEN IN THIS RESEARCH
Framed from a state, government and private-sector focus on cybersecurity	A focus on the sociocultural contexts, such that the unique cybersecurity landscape and role of WCSOs and WHRDs within national, regional and global contexts
Techno-centric focus on cybersecurity	A human-centric focus that expresses cyber functioning, resources, vulnerabilities, threats, responses and harms in human-centred terms
No or limited focus on embedded gender biases in cybersecurity	A gendered lens on cybersecurity that recognizes the personal, social and environmental factors that impact women's (and their advocates') cybersecurity
Mitigation of cyber risks and recovery from cyberattacks	A cyber resilience focus that emphasizes a holistic approach including proactive preparation, reduction of impacts and recovery from cyber threats, and management of cyber risks with the aim of promoting adaptive responses

2.2.1 ANALYTICAL FRAMEWORK

This research employs an analytical framework that draws on socio-technical characterizations of cyber-security while allowing space to explore the gendered implications of these concepts. The framework identifies four key concepts that are the focus of this study and with which the results are organized: cyber assets, cyber threats, cyber vulnerabilities and cyber resilience (see Table 2).

TABLE 2. KEY CONCEPTS UNDERPINNING THE ANALYTICAL FRAMEWORK

CONCEPT	DEFINITION	EXAMPLES
Cybersecurity Assets	All types of technology and its affordances that are used to support personal or organizational functioning, to produce value or to achieve goals. These include tangible (physical) and intangible (nonphysical) assets	*Tangible:* › Devices/hardware (e.g. laptops, PCs, phones) › Network infrastructure *Intangible:* › Data › Intellectual property › Brand or reputation › Partnerships
Cyber Threats	Broadly adverse cyber incidents that have the potential to cause harm to individuals, organizations and entities through technological systems and the way they are used, e.g. by compromising the functional capacity of assets, via exploiting cyber vulnerabilities or by leveraging social and psychological vulnerabilities.	› Data breaches or security violations where information is stolen, altered or used without permission › Doxxing or intentional sharing of personal information › Malware or software intentionally designed to cause disruption (e.g. ransomware, spyware and viruses) › Online harassment and threats, including bullying, trolling, and hate speech › Social engineering attacks where individuals are manipulated into performing actions or divulging confidential information (e.g. phishing)
Cyber Vulnerabilities	Weaknesses, both technical or non-technical, that can exacerbate the harms caused or the likelihood of exploitation and exposure to cyber threats	› Using the same devices or accounts for professional and personal purposes › Outdated devices or software that lack current security updates › Lack of digital literacy and technical skills › Social and cultural norms › Inadequate policies and procedures › Lack of legal protections
Cyber Resilience	The state of, or dynamic process in which, an individual, organization or entity can effectively maintain continuity or enhance operations through the prevention, disruption and mitigation of cyber threats with the result of minimizing harm[33]	› Planning and preparing for both known and unknown cyber threats › Assessing and mitigating against technical and non-technical vulnerabilities › Having pre-existing procedures and response strategies against cyber threats › Learning from cyber incidents to enhance cybersecurity practices

33 Hausken, K. (2020). Cyber resilience in firms, organizations and societies. Internet of Things, 11, 100204.

This project adopts the concepts outlined in Table 2 in order to better understand the cybersecurity posture and the degree of cyber resilience among WCSOs and WHRDs in Southeast Asia. Specifically, it investigates:

1. Digital assets, focusing on the roles, affordances and uses of digital technologies in achieving individual and organizational goals;
2. The perceptions and experiences of organizational and personal cyber threats;
3. The vulnerabilities that may exacerbate the likelihood of adverse cyber threats; and
4. Narratives of cyber resilience whereby individuals and organizations seek to prevent, disrupt and even grow from adverse cyber events.

It is important to note that threats and vulnerabilities are interconnected and often reinforce one another, creating a complex web of challenges for WCSOs and WHRDs online. Addressing these requires a comprehensive approach that takes into consideration the complex interplay between these issues in the context of women, peace and cybersecurity.

2.2.2 RESEARCH QUESTIONS AND METHODS

This report addresses two main research questions:

> **Research Question 1:** What is the cybersecurity posture of WCSOs and WHRDs in Southeast Asia?

Research Question 1 includes three critical sub-questions:

1. What cybersecurity assets do they have, and how are these utilized?
2. What cyber threats do they commonly experience, and how are these perceived?
3. What cyber vulnerabilities do they have?

> **Research Question 2:** How cyber-resilient are WCSOs and WHRDs in Southeast Asia?

These questions will be analysed from a peace and security lens in order to assess their implications for the implementation of the WPS agenda in Southeast Asia.

To address the research questions, a mixed-method approach was undertaken. First, a review of the literature and relevant national cybersecurity indicators was undertaken to situate the research in the Southeast Asian context.[34] (See Appendix 1 for further detail on the methodology and Appendix 2 for a detailed outline of the cross-national review.) Second, quantitative and qualitative primary data were collected. Specifically, 80 participants currently working in a CSO or WCSO completed an online survey and 21 WHRDs were interviewed. An explanatory sequential triangulation design was used to analyse the data; the quantitative data was analysed and evidence from the qualitative data was used to build depth and nuance in the findings and their interpretations.

Digital assets, cyber threats, cyber vulnerabilities and cyber resilience are investigated in this study.

34 The countries surveyed in the primary data collection include Cambodia, Lao PDR, Myanmar, Philippines, Thailand and Viet Nam. Secondary data collection focused on the Southeast Asia region as a whole, including all 11 ASEAN Member States as of August 2023. For more information, see Appendix 1.

3.

THE CYBERSECURITY POSTURE OF WCSOS AND WHRDS IN SOUTHEAST ASIA

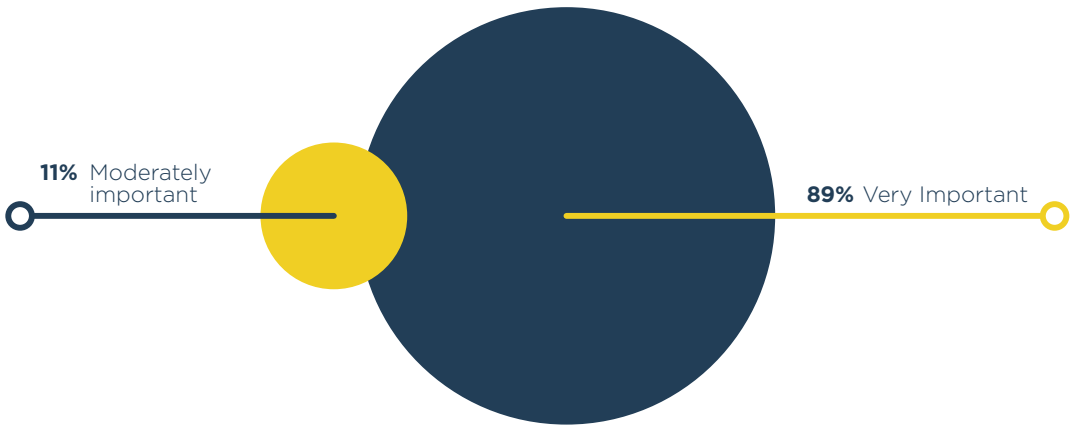
Digital technologies have the potential to facilitate and transform civil society's and human rights defenders' work in numerous ways, as reflected in the growing research on ICTs for Development.[35] There is now well-established literature in this area that illustrates the importance of digital technologies for CSOs, from extending information-sharing and outreach to community building, fund-raising and service delivery.[36] This may be even more central in the context of human rights defenders, where digital technologies provide new mechanisms to engage in advocacy and activism, including peace efforts, and in which these platforms are more accessible than ever to a diversity of potentially marginalized voices. Technology has the potential to support community organizations and advocates in fulfilling their missions, becoming more sustainable and building social cohesion. This research found similar results, with technologies not only being important but also seen as a central element of operations.

3.1 Tangible and Intangible Digital Assets

3.1.1 THE IMPORTANCE AND USAGE OF DIGITAL DEVICES

Tangible assets are the physical resources owned or operated by an organization that support the functioning of an individual or organization, such as digital devices (e.g. laptops, phones, servers), systems and network infrastructure. The large majority of WCSOs (89 per cent) indicated that digital technologies (i.e. tangible digital assets) were very important for their work.

FIGURE 1. IMPORTANCE OF DIGITAL TECHNOLOGIES FOR WCSOS



35 Walsham, G. (2017). ICT4D research: reflections on history and future agenda. *Information Technology for Development*, *23*(1), 18–41. https://doi.org/10.1080/02681102.2016.1246406

36 Lynn, T., Rosati, P., Conway, E., Curran, D., Fox, G., & O'Gorman, C. (2022). Digital Technologies and Civil Society. In Digital Towns: Accelerating and Measuring the Digital Transformation of Rural Societies and Economies (pp. 91-108). Cham: Springer International Publishing.

The WHRD interviews provided additional insight into why these assets were so important, with some indicating that their work was now synonymous with the technologies that they use, particularly as a result of the major changes brought about during the COVID-19 pandemic.

"Technologies and the applications that we use are definitely important to us because that is how we function as an organization. That is how we do our work and advocacy."

"While we are adjusting and were able to cope [with change]. We didn't think that these digital tools would also enable us to continue to do our work. I mean, for the past two years, we're heavily dependent on online and social media."

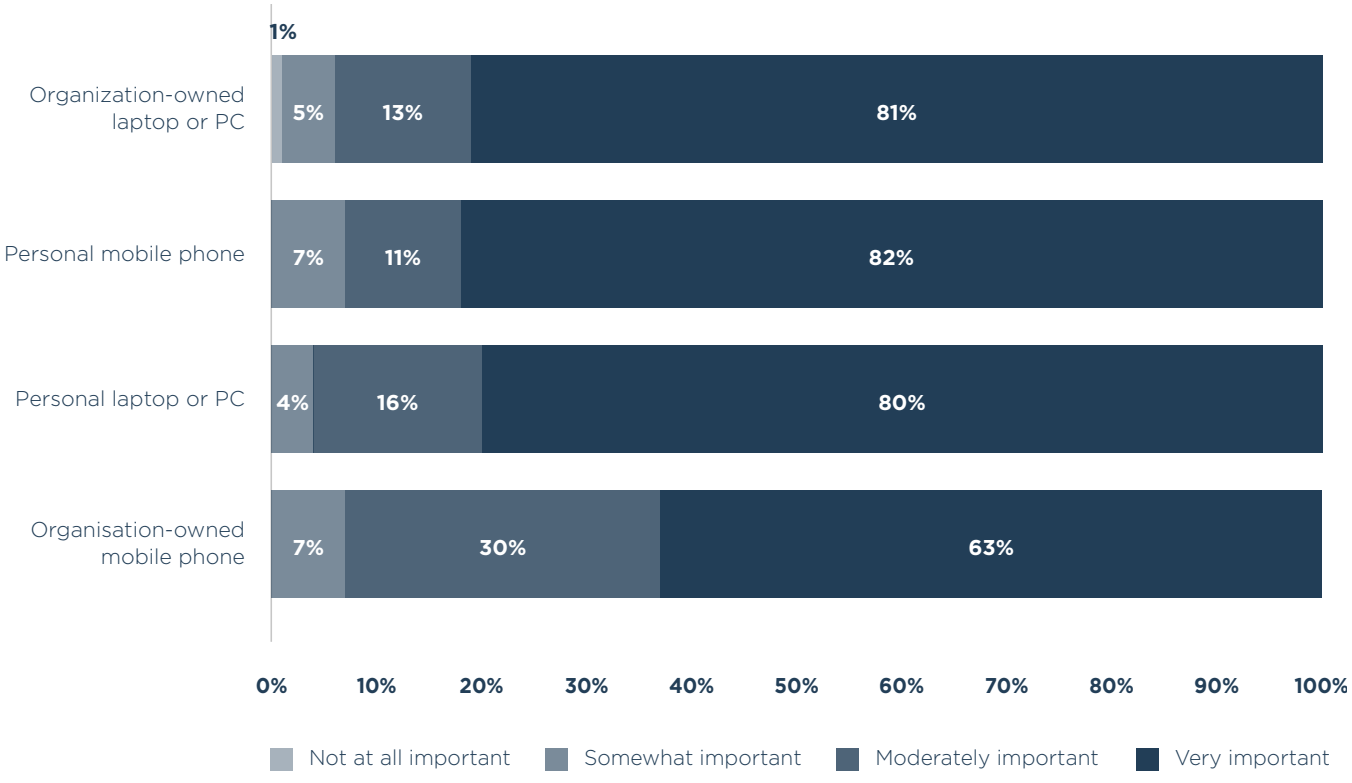
One of the interviewees highlighted that technologies are *"like our life, the life of the work,"* that provide critical avenues for connecting with service beneficiaries, calling for action among the broader community and supporting all elements of day-to-day operations. Interviewees identified a variety of types of assets that have critical work-related functions, including website management, human resources, data capture mechanisms, payments systems, applications to produce and disseminate content (such as infographics, podcasts and video content), platforms to collect, store and share information and data, and mechanisms for connection and collaboration (see social media section below for more detail).

One interviewee worked as part of an organization that supported those with diverse disabilities. In this context, technologies were not only critical for the functioning of the organization but also assisted in creating meaningful opportunities for those with intersectional vulnerabilities. These tools have enabled people to thrive in ways that were otherwise inaccessible without the use of technology.

"They could not feel their disability because they can communicate. They have access to information and job opportunities, and their disability doesn't matter because they are being measured by the outputs that they give, not their disability. So this digital technology is a breakthrough."

In terms of the devices used, the majority of survey participants (78 per cent) accessed an organization-owned computer and a personal mobile phone (71 per cent), with a minority having access to a work-owned mobile phone as well (34 per cent). 61 per cent of the participants used a personal computer for work purposes as well, but most had access to organisation-owned computers and thus this tended to do so to supplement their work access (e.g. home-based or field work). A small number of survey participants (n=18) lacked access to any work devices, relying instead entirely on their personal computers and mobile phones.

FIGURE 2. IMPORTANCE OF DIGITAL DEVICES FOR WORK (N = 80)



The importance of technological affordances such as convenience, privacy and safety were consistently mentioned by interviewees in the preference of tangible assets. A key insight was that personal devices were seen to be equally as important for work as those owned by one's organization. This finding was corroborated by participants who related that beyond their laptops, the most important piece of technology in their work was a mobile phone. The reasons for this importance included the convenience and accessibility of engaging in work where there were very fast turnaround times and collaboration/ connections with others was paramount; *"My phone, because always in my hand and fast distributing information"* and *"My mobile phone - in our work, we need to go to the communities, to coordinate."*

Personally owned devices are often not within the security remit of organizations, and thus tend to not be covered by organizational policies or regulations. As quoted by two of the interviewees:

"The main [cyber vulnerability] really lies in use... there are some who are still using personal devices where official documents are stored. It's where the vulnerability comes in. But I believe it's more on the user, there is a problem with the user more than the infrastructure."

"This is a problem of type people who do not distinguish between work and something like private life. And they use work methods of communication like they use for private."

Another potential risk is that stolen or confiscated personal devices may expose the private information of friends and family.

3.1.2 SOCIAL MEDIA: APPLICATIONS AND USAGE

The term 'social media' refers to a range of digital platforms and technologies that enable individuals and groups to publicly and privately create, share and exchange information, ideas and content with one another. An emerging body of research suggests that social media is a critical digital asset that can empower grass-roots communities by allowing them to produce and disseminate information and media, thus providing avenues to form groups and drive social movements.[37, 38]

Individuals and groups can generate public attention through social media, reducing reliance on mainstream dissemination channels and bypassing the many barriers and potential biases inherent in these.[39] Social media also enables networked connections across boundaries and borders, assisting in both instrumental support (e.g. funding, human resources) and social support, effectively making it easier for community and civil society groups to form sustainable coalitions.

The possibilities of 'mass mobilization', where there is easy and rapid dissemination of knowledge and the ability to form supportive relationships among those with a common agenda, supports collective activism.[40] Indeed, social media can empower civil society and local communities, fulfilling many different participation needs by allowing their voices to be heard by many and supporting social mobilization.[41]

As for the importance of social media, research findings revealed that 71 per cent of survey participants used social media for work, with 82 per cent believing that this was very or moderately important to their work. In addition, the majority of survey participants (81 per cent) used social media for personal purposes (note that 36 per cent did not separate personal from work social media). **Interestingly, those in WCSOs (73 per cent) were more likely to keep personal social media separate than those in CSOs (61 per cent)**.

When asked what was the most important digital technology used in work, social networking platforms and messenger applications were seen to be of high importance, although less important than a personal computer or mobile phone overall. Interviewees confirmed these findings; the majority mentioned using social media in some form, with two critical features (external and internal communications) and associated platforms reiterated consistently.

First, social media was used to engage in external communications and outreach in mass personal or public ways through social networking platforms like Facebook, Instagram, X (formerly Twitter), and YouTube. These were seen as key ways to garner support for social movements and as ways to counter misinformation and disinformation.[42]

37 Fuentes, M.A. (2007). Digital Activism, in the *Encyclopedia of Activism and Social Justice*, G.L. Anderson and K.G. Herr (eds.). Thousand Oaks: SAGE Publications, Inc.
38 Kane, G. C., Alavi, M., Labianca, G., & Borgatti, S. P. (2014). What's different about social media networks? A framework and research agenda. *MIS quarterly, 38*(1), 275-304.
39 Yuce, S. T., Agarwal, N., Wigand, R. T., Lim, M., & Robinson, R. S. (2014). Bridging women rights networks: Analyzing interconnected online collective actions. *Journal of Global Information Management (JGIM), 22*(4), 1-20.
40 Enjolras, B., Steen-Johnsen, K., & Wollebaek, D. (2013). Social media and mobilization to offline demonstrations: Transcending participatory divides? *New media & society, 15*(6), 890-908.
41 Alizadeh, T., Sarkar, S., & Burgoyne, S. (2019). Capturing citizen voice online: Enabling smart participatory local government. *Cities, 95*, 102400.
42 Notably, the ease with which information is accessed and disseminated on social media has also made it a key contributor to the spread and perpetuation of misinformation and

By producing content that was hosted on globally connected spaces, it was recognized that messages would have greater reach and, thus, higher impact.

"Yes, so for Facebook, I'm most likely to use it for the impact or the result of our work and also for branding, to reach out to more audiences and also connect with those who are known so they can also see our activity from time to time."

Of note, social media was also a mechanism to gather volunteers for activism causes. The importance and utilization of social media for these purposes is complex and multilayered, with the following quote illustrating the intentional use of public platforms as a way of connecting supporters into more private functions of social networking:

"We recruit volunteers from Twitter. Twitter is a channel to draw volunteers to [private] Telegram and Line groups."

The quote above highlights a second key feature of social media — the use of private groups and direct messaging to connect individuals and groups privately and safely. These features also provide a vehicle to offer support to those who need quick and easy ways to connect.

"They can share whatever sentiments they have in the [social media] community because it's... a private group. So it's easier for them to share whatever they want to share without, you know, any hesitations [or potential repercussions]. "

"Most of my personal social media accounts are active, so I always encourage [women in need of support] to send me a message if they have any questions or if they have any concerns."

As per the previous section, where technologies were understood to be the cornerstone for civil society operations, social media was found to be highly functional in enabling safe communications both internally (among team members and collaborators) and externally (with those who were supported by the WCSOs and WHRDs). For both of these communicative functions, the three main applications discussed were Signal, Telegram, and WhatsApp. Notably, encryption (also known as secure messaging) was seen as a critical feature in each of these applications. Encryption is the process of encoding information to prevent anyone other than its intended recipient from viewing it. In some applications, it is only the text of messages that are encrypted, whereas in others, this also applies to phone calls made and files and images sent through the apps.

Encryption was highlighted as a feature that promoted feelings of safety, protection and confidentiality, especially when working with vulnerable people or sensitive topics. As one interviewee mentioned when talking about a group they were supporting who lived in a remote region, *"working in the forest in jungle areas, the only safe app that they could use was WhatsApp. All the other apps were being tracked, and they had to use encrypted messages."* More often, though, Signal and Telegram were discussed as providing secure, encrypted communications. *"Yes, we use Signal with some of the groups that we work with; we feel that it is more secure compared to [other platforms]."* One of the reasons for this was because of the lack of trust in the large tech companies that run many of these applications. As highlighted by one interviewee, some of the issues with the companies came from the fact that they did not have users' best interests at heart and put profit first: *"They are the business, right? The Signal is like NGO, you know, is nonprofit."* But as aptly mentioned by another, the use of these applications was a "trade-off."

"I don't think [this platform] is really safe, but compared to [others] it is... Signal is a little bit better, but it's not easy to use. So it's kind of a trade-off when we talk about the security and then the functionality."

Another interviewee mentioned that they were "not comfortable" using a local messaging app due to its technical insecurities as well as a known relationship with the government. Thus, when they came into a position of power in their organization, they changed operations to Signal. This change had the added benefit of slowing down communications and making people more thoughtful about what they shared, as the app was unfamiliar and not used by people for their day-to-day communications.

"Plus, you don't just talk about something like joking around or saying good morning, or sending some random stickers, that's something that we don't do when we use the Signal app...[but] if there's something very urgent, we use the other app to get in touch. But we always know that if it is something important, dangerous, risky, we are not going to put that in [the unencrypted app]. "

disinformation, and these platforms are also they main way this is being thwarted by WCSOs and WHRDs.

While encrypted applications were preferred and thought to offer greater security, the failure of safety mechanisms on messaging applications (outlined in later sections) is notable due to the difference between perceptions of what encryption offers as compared to what it actually offers.

For example, Salter[43] suggests that while communication applications may state that they are encrypted, some collect and potentially use non-encrypted pieces of metadata about senders' and receivers' devices. Also, encrypted apps are of little help if mobile devices are stolen or applications hacked, unless the device itself is fully encrypted.

Furthermore, because some of the applications that were perceived to be more secure were not used in other areas of life (e.g. for mundane communications), switching between many apps to achieve desired outcomes was experienced as a barrier — particularly by those with lower levels of digital skills or those who were used to using less secure applications. This issue was suggested by one interviewee as having somewhat of an inconsistent effect, such that it negatively influenced those who were older (who were less likely to use many different apps) as well as those who were younger (who were unwilling to compromise connectivity for safety).

Just as switching between and across different social media applications was a way that WHRDs could protect their safety and minimize cyber risks, another interviewee discussed dynamically utilizing public and private groups in a similar way.

"We will also create new Telegram groups for each action or event, talk inside that, and delete the group after we finish the action... After that, we go back to the role-based Telegram groups again: public relations, core team, finance, specific issues, etc. But they are all scattered, so we map all of these to communicate across them in the groups."

The quote highlights that the grouping function within Telegram was deliberately used to create separation as well as to assist in overall integration of those involved in the movement. This helped the organisation to maintain security by ensuring that only known and trusted individuals were included in groups where there was sensitive information shared. This was particularly important for the interviewee in light of previous experiences of infiltration by non-legitimate group members who gathered information about activities to undermine and disrupt protest movements. The functionality also helped group moderators understand which members of the online group would be more or less likely to become key members of their movement as they were able to watch and monitor interactions within the group; *"we will follow them as we see them as having potential."*

In summary, the role of social media is incredibly important and very complex in terms of cybersecurity for WCSOs and WHRDS, as highlighted by the following quote:

"[Social media is] important in terms of amplifying what's happening on the ground, so you're using it for blogs, for quick posts, for soliciting support, all of those forms that are really important. But I would delineate those platforms, like Facebook and LinkedIn, Instagram and Twitter, as being ones that are outward facing where we're trying to mainstream gender and enlist support from a broad public audience in different countries and communities. But we also use social media to communicate with WHRDs; because of the encrypted message system, we are able to communicate safely... I worked with women activists who had created a kind of underground communication system, using something similar to WhatsApp, so that they could share information about where there were threats and where there were safe houses. So yeah, having those safe communication systems is just so vital for WHRDs when they're facing terrifying threats."

3.2 Cyber Threats

A cyber threat is any situation that has the potential to cause harm to individuals, organizations or entities through technological systems. It also includes the exploitation of technical, social and/or psychological vulnerabilities. A cyberattack is a type of action that involves a malicious act against a person, organization or nation, violating its security and causing damage.

As the technologies and applications used by organizations and their employees have multiplied, cyber threats have become increasingly complex. In this context, threat actors are using sophisticated tools to target a variety of

43 Salter, J. 2021, 8 September. WhatsApp "end-to-end encrypted" messages aren't that private after all. Ars Technica. https://arstechnica.com/gadgets/2021/09/whatsapp-end-to-end-encrypted-messages-arent-that-private-after-all/

FIGURE 3. WCSOs PERCEPTIONS OF COMMON CYBER THREATS

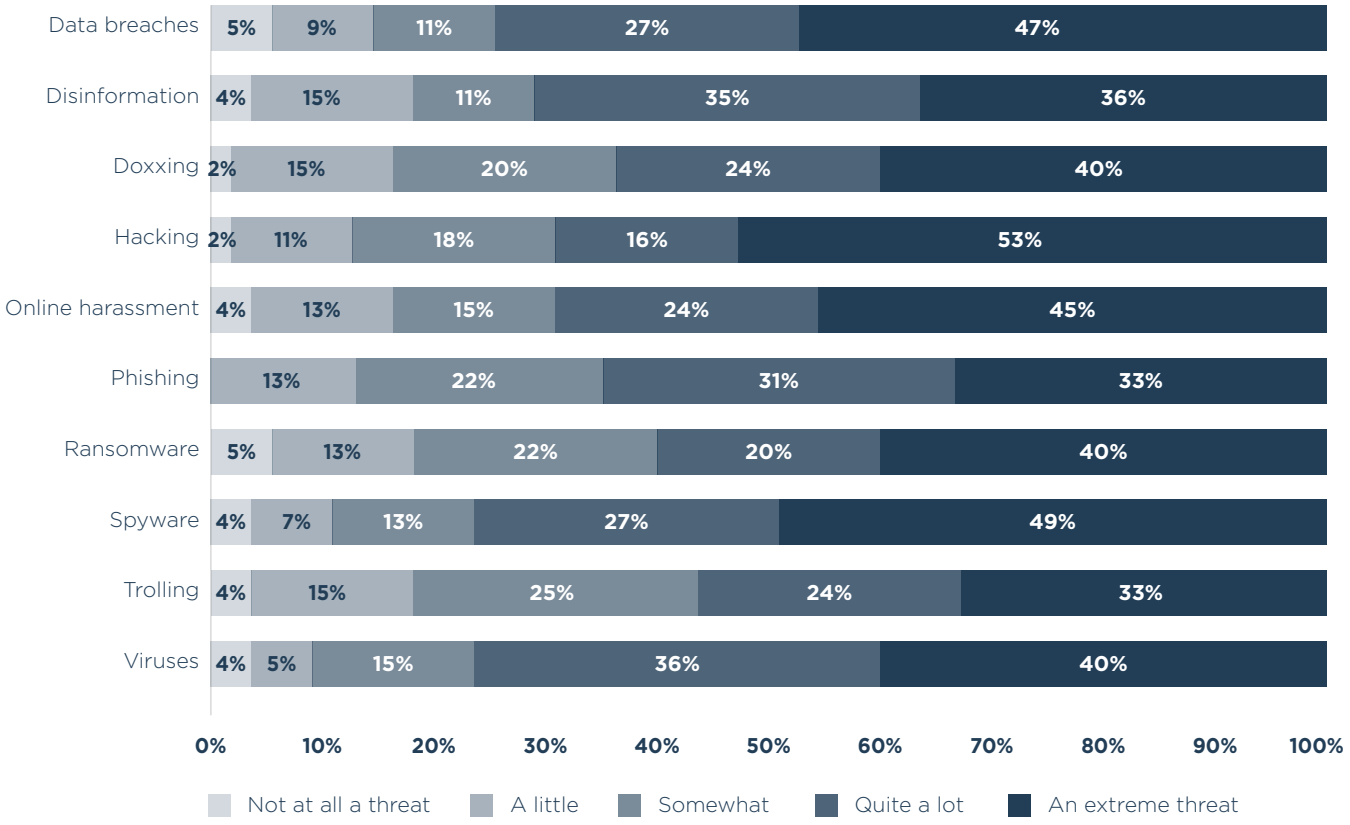


FIGURE 4. CSOs PERCEPTIONS OF COMMON CYBER THREATS

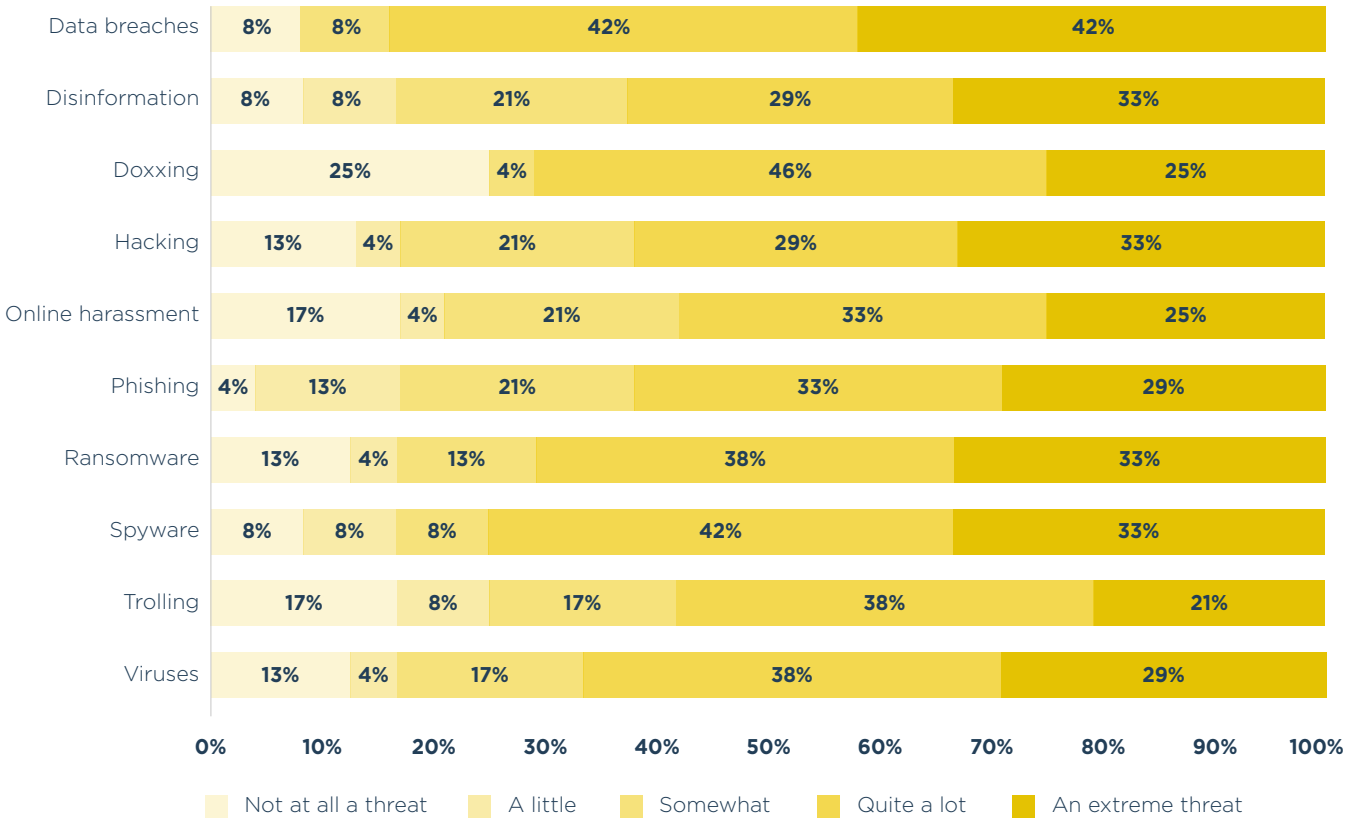


FIGURE 5. WCSOs EXPERIENCES OF COMMON CYBER THREATS

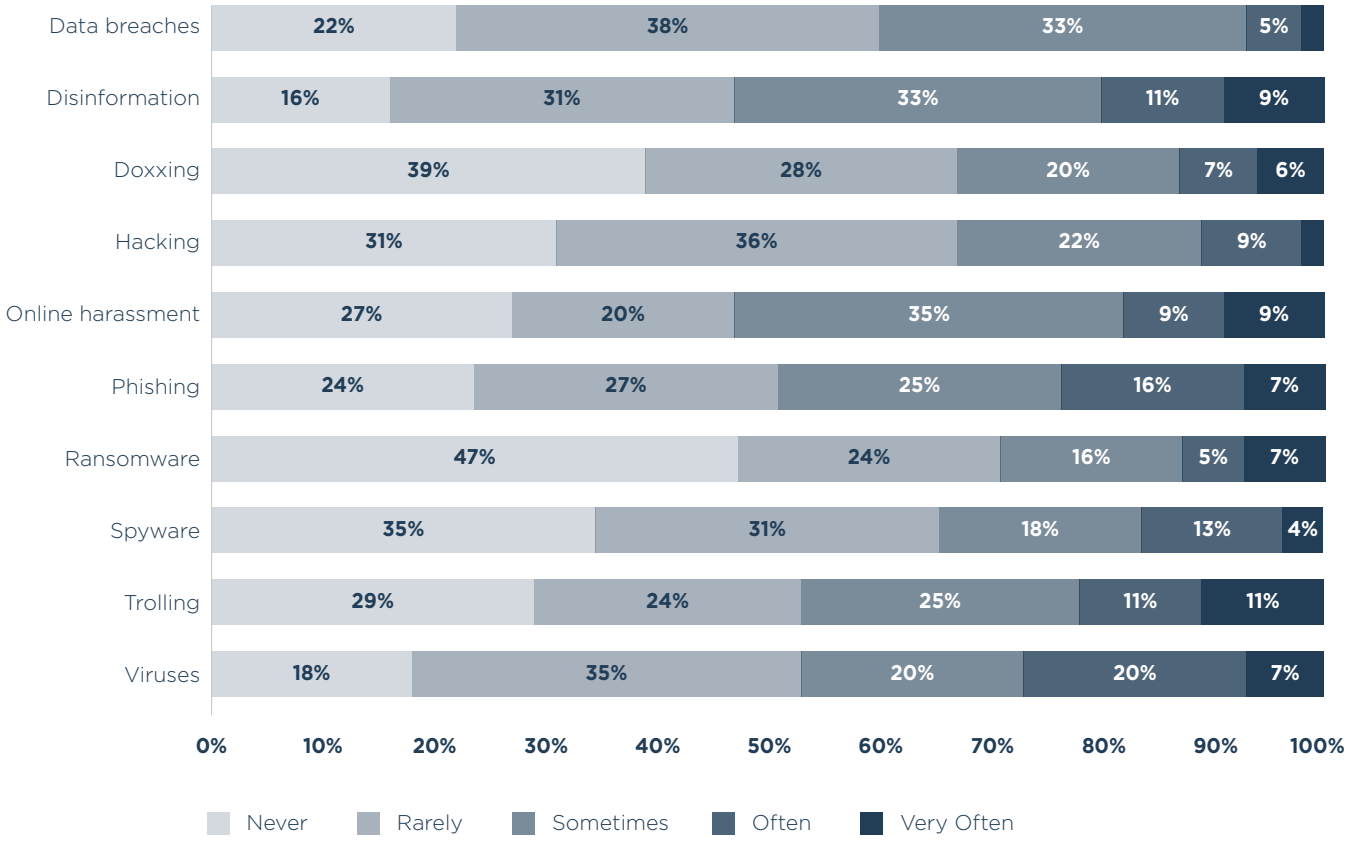
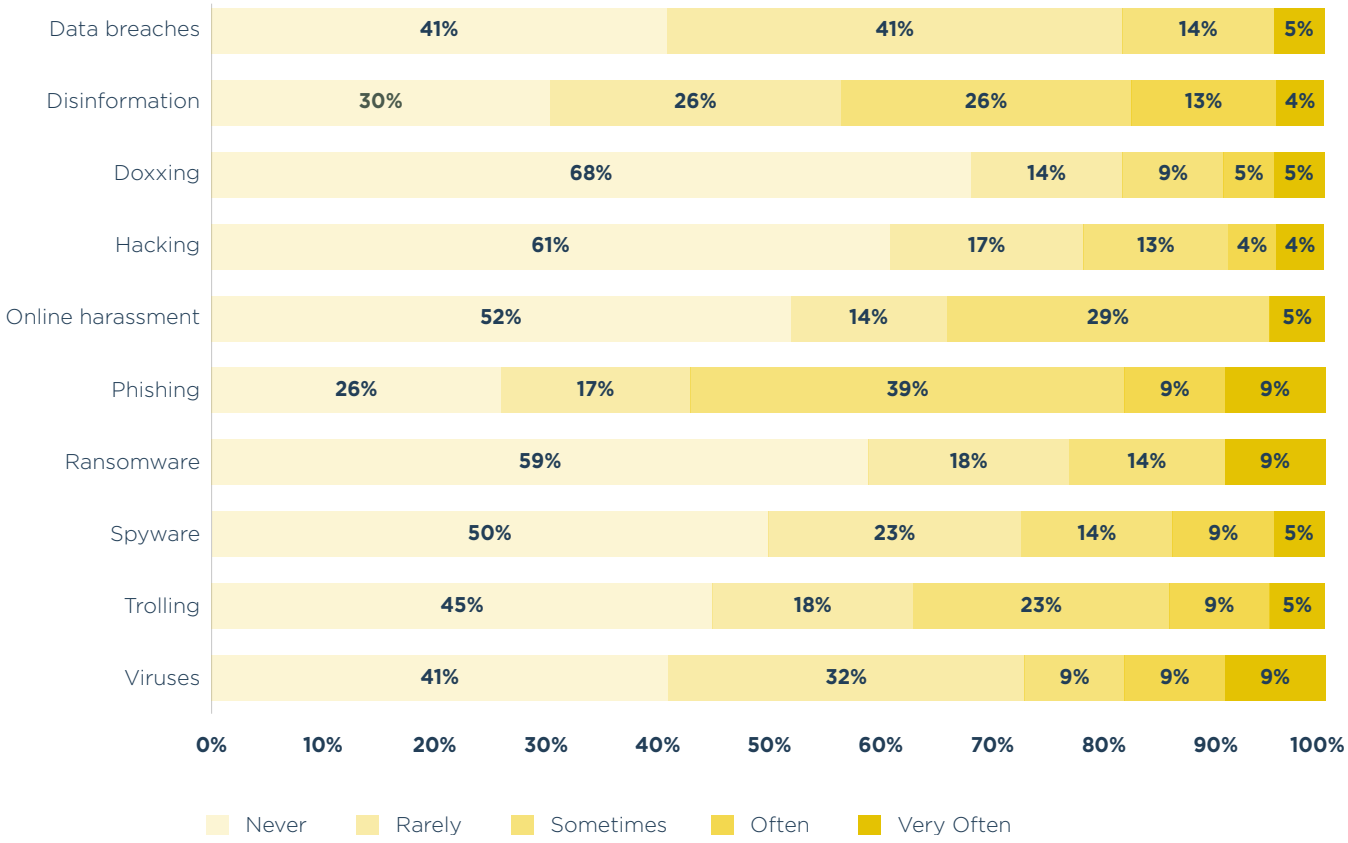


FIGURE 6. CSOs EXPERIENCES OF COMMON CYBER THREATS



devices, systems and applications; . Furthermore, as the tools are becoming more advanced, they are easier and more accessible to a wider range of individuals and organizations. For instance, AI-driven techniques (labelled as AI-based cyberattacks) are now being used alongside conventional attacks to cause greater damage. Some examples of this include next-generation malware that can continuously update itself to remain undetected and bypass mitigation measures, synthetic media technologies that can be used for impersonation and disinformation, including voice synthesis technologies that mimic real speech or convincingly impersonate a real person, social bots that generate fake reviews and comments, and many other potential yet unknown applications.[44]

These rapid developments in technologies and attack tactics, techniques, and procedures make new threats difficult to detect and prevent, thus making it easier for threat actors to exploit vulnerabilities and harder for potential targets to maintain security. It can be very difficult to undertake an effective threat assessment, especially given that lower-level threats are often specifically crafted to create pathways for more substantial malicious attacks in the future. Furthermore, the increasing adoption of digital technologies in everyday life - particularly the proliferation of insecure "Internet of Things" devices (such as Internet connected cameras, monitors, and door locks), and the intertwined use of personal technologies for work purposes has increased possible attack vectors across devices and contexts, blurring the line between individual-level threats and those experiences by organizations. Therefore, this research took a broad approach to cyber threats, first by examining the perceptions and frequency of threats as experienced within organizations (by individuals or the whole organization), and second by examining personal experiences of threats.

3.2.1 ORGANIZATIONAL CYBER THREATS

This research measured cyber threats that were identified as common for WCSOs during the literature review. These cyber threats are listed in brief detail in Table 3 and include broad issues related to technical security, such as malware (software and applications that are designed to disrupt devices, gain unauthorized access to information or interfere with security and privacy) and socio-technical threats, such as online harassment. In measuring cyber threats, a definition was provided for each incident, and individuals were asked about their perceived level of threat and the frequency with which these threats took place in their organization (personal threats were also assessed and discussed in section 3.2.2). Comparisons of threat perceptions and experiences across those in the sample categorized as CSOs (n = 24) and WCSOs (n = 56) were undertaken where appropriate and relevant (note: given the differences in sample sizes comparisons made should be treated with caution).

TABLE 3. PREVALENCE OF ORGANIZATIONAL CYBER THREATS

CONSTRUCT	DEFINITION	THREAT PERCEPTIONS		THREAT FREQUENCY	
		CSO Mean	**WCSO Mean**	CSO Mean	**WCSO Mean**
Data breaches	Any event that exposes confidential, sensitive or protected information	4.08	**4.04**	1.82	**2.14**
Disinformation	False information spread over digital media intended to mislead or spread rumours	3.71	**3.81**	2.35	**2.56**

44 Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR), 53(1), 1-34.

CONSTRUCT	DEFINITION	THREAT PERCEPTIONS		THREAT FREQUENCY	
Doxxing	Private or identifying information distributed about a person on the Internet with negative intent	3.46	**3.73**	1.64	**1.99**
Hacking	Unauthorized access to or control over computer network security systems for an illicit purpose	3.67	**3.95**	1.74	**2.03**
Online harassment/ threats	Targeted towards individuals or the organization	3.46	**3.80**	1.86	**2.56**
Phishing	Malicious communications designed to trick people into falling for a scam, divulging sensitive information or taking other action against their or their organization's interests	3.71	**3.81**	2.57	**2.34**
Ransomware	Malicious software designed to block access to a computer system until a sum of money is paid	3.75	**3.76**	1.73	**1.94**
Spyware	Malicious software designed to enter your device, gather data about you, and forward it to a third party without your consent	3.83	**4.11**	1.95	**2.13**
Trolling	Deliberate attempts to offend, inflame, attack or provoke	3.38	**3.67**	2.09	**2.39**
Viruses	A computer program that can self-replicate, infect other programs, and spread to other computers	3.67	**4.04**	2.14	**2.49**

Threat perception scale range: 1= not at all a threat – 5 = an extreme threat
Threat frequency scale range: 1= never - 5 = very often.

Figure 5 and Figure 6 show that people from both WCSOs and CSOs rated the majority of issues presented as being of a high of threat, i.e., there were high levels of threat perception and participants were aware of the risks posed by technology. This is contrary to other research in the area, which suggests that a lack of awareness of the harms of cyber threats is a critical reason for poor cybersecurity practices, especially among those who are not experts in digital technologies. This is a very important insight, as the current narrative of capacity

building is predominantly focused on knowledge acquisition, whereas it may be more effective to focus on strategies and practices to minimize and mitigate the impacts of these threats.

The threats perceived to be the most impactful (reported as either "quite a lot" or "an extreme" threat) were data breaches (WCSOs = 74 per cent, CSOs = 84 per cent) and spyware (WCSOs = 76 per cent, CSOs = 75 per cent). The least impactful threats were trolling (WCSOs = 57 per cent, CSOs = 59 per cent). There was a range of differences between WCSOs and CSOs, the most notable was that there were higher on average threat perceptions on almost all of the indicators (further outlined in Table 3).

Participants were also asked if they experienced any threats that were not listed. The only issue that was uniquely mentioned in this "other" category was distributed denial of service (DDoS) attacks (mentioned by three survey participants), in which attackers seek to make digital resources unavailable to and unusable by legitimate users by disrupting or flooding services of a host connected to a network.

Figures 7 and 8 outline the frequency with which participants indicated they had experiences of organizational-level cyber threats. As outlined previously, these results show different patterns of responses compared to the perceived impact of threats. Specifically, when defined as those threats that had been experienced occasionally or more often, phishing was the most common occurrence for CSOs (57 per cent), whereas disinformation and online harassment were the most common for WCSOs (both 53 per cent). Ransomware and doxxing were the least commonly experienced cyber threats, but these were more likely to have been experienced by those in WCSOs as compared to CSOs.

The results indicate that some of the incidents with the lowest threat perceptions were experienced the most frequently. This is not unexpected, as disinformation, phishing and trolling are very common, widely discussed and easy to initiate types of cyber threats. Yet, from these results, it is unclear whether these threats were considered less impactful because organizations have better safeguards against them or whether the impacts of these threats were generally considered to be less severe. Further, just because they were not perceived as highly threatening does not mean that these threats are not harmful to WCSOs and WHRDs, as both phishing and trolling have been found to have important negative outcomes for individuals and organizations and are possible inroads for major cyber incidents.

A critical finding is the high frequency with which all threats were experienced by WCSOs. Even the lowest rated, ransomware, had been experienced by 53 per cent of WCSOs. Furthermore, the incidents rated as the most threatening (disinformation, data breaches, spyware and viruses) were all experienced by more than one-third of WCSOs, or sometimes more.

As per the results above, trends indicate that WCSOs have higher threat perceptions than CSOs, with the largest differences evident for viruses and online harassment (See Table 8 for full information). These findings also suggest that, on average, WCSOs have a higher frequency of cyber threats, with the largest differences being for online harassment, trolling and doxxing.

Although the interviews predominantly focused on individual-level experiences of cyber threats, there were also two distinct types of organizational-level cyberattacks that were mentioned: cyber-bombing and impersonation.

Cyber-bombing is a type of harassment in which an individual or a group of unwanted and uninvited users interrupt online meetings and events, often to intentionally disrupt and incite hate. This type of cyberattack is also known as Zoom-bombing or Zoom-raiding, terms that came into common parlance due to the increasing use of (and security problems with) the Zoom videoconferencing service during the COVID-19 pandemic period. These types of cyberattacks can be very difficult to prevent; research has found that almost all targeting happens in real-time, is opportunistic and is not sensitive to normal protective strategies (such as password protection), so there is little or no time to prepare.[45] During the interviews, three different experiences with such attacks were mentioned, all of which were related to events and meetings that supported a feminist agenda.

"It's happening to not just me, but friends and local organizations, leaders that I know, like daily hits - it's not just something that's happening irregularly, it's happening on a very regular basis... [this is prevalent when] organizing feminist conferences, where there isn't

45 Ling, C., Balcı, U., Blackburn, J., & Stringhini, G. (2021, May). A first look at zoombombing. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 1452-1467). IEEE.

security, where it's a more open invitation to people to join... Most recently, when organizing a gender equality conference... they organized it to be as open and inclusive of different voices as possible. And because it wasn't organized as an invitation-only event, it meant that it was very easy for those who were against any form of gender equality and seeking to disrupt the convening. They were able to just bomb the site with messages so that the whole site for the conference went down, and the organizers had to cancel the rest of the conference."

"Because they were holding an online women's empowerment conference, they experienced that someone, an unauthorized person, entered the event and shared their screen... So they stopped the session, and when they went back to the session, it repeated, so they ended up cancelling that event on that day. Basically, this acted to really undermine the event itself... which was really promoting women's empowerment."

These quotes highlight similar sorts of cyber-bombing incidents and associated outcomes, where the underlying issue identified was a lack of protections put in place to stop unauthorized entry. These interviewees went on to discuss how future events put password protections, registrations and locked screen sharing in place, which indicates types of cyber resilience (discussed in subsequent sections). However, research has found that some of these protections can be ineffectual, especially with targeted attacks where perpetrators share passwords on social media for such events or pose as legitimate attendees by using faking names and affiliations.[46, 47] Furthermore, the disruption caused by cyber-bombing may diminish the actual experiences of those who are targeted, as outlined by another interviewee:

"The day our event poster came out and was published on Facebook, the anti-feminist group shared this poster, and they asked each other to come to this Facebook Live and... they just bombarded it with hate speech in the comment section in real-time. There were more than 500 comments to try to discredit [the speaker], sexually harassing comments, sexist comments, everything."

The content, extent and violence of the cyber-bombing in the above quote are more apparent than in other instances discussed. Additionally, this type of cyber-bombing is related to another activity that has variously been called touring, hate-raids and flooding, in which a user or group is barraged (generally through social media) with direct messages, tags, comments or negative reviews to such an extent that this disables functional use of the application. Examples are provided in the quotes below:

"My page also got targeted by some anti-feminism people; they just came to my page and said this page is bad and just put one star. That's why my page rating just dropped ... I did not care about that, but this is how they try to discredit us in any way."

"[A leader] for gender equality had a kind of a cyber bombing of hate messages via apps that just bombarded her. So it seems in many feminist spaces at the moment, there is kind of targeted attempt to really disrupt, damage and destroy a lot of the organizing and the advocacy for women's rights and injustice."

"So basically, they just bombard your page with a lot of tags and with that large number of posts to make your operation more difficult. Because you get overwhelmed and cannot ignore them. When they tag us, there's a notification, and when we go to read it, it is something about rape, or a meme that is very harmful, or something like that. It's sexual harassment."

Although each one of these examples is slightly different, they all highlight the wide-ranging harms that result from these incidents: **being discredited, creating extra work under conditions of scarce resources and exposure to hate speech, misogynistic content and sexual harassment**.

The second distinct type of cyberattack mentioned in the interviews was impersonation, where spoof, parody, fake or impostor accounts were created and maintained. These were typically focused at the organizational rather than the individual level. These accounts copied the identifying brand features of the organization in order to undermine its aims and messages. Two of the interviewees currently had active impostor accounts on social media fraudulently posing as their organization. Both discussed the sophisticated use of imitating brand imagery to fool potential followers so that they could spread misinformation or hate content:

"They're pretty [convincing] and they have learned the way that we use our corporate identity. So, the font is not correct, but the colour is correct. The pictures they use,

46 Lee, C. S. (2022). Analyzing Zoombombing as a new communication tool of cyberhate in the COVID-19 era. *Online Information Review, 46*(1), 147-163.
47 Lee, C. S., & Jang, A. (2023). Sharing Experiences and Seeking Informal Justice Online: A Grounded Theory Analysis of Zoombombing Victimization on Reddit. *Victims & Offenders*, 1-20.

the way they post, the language they use. It's all to try to imitate us and a lot of people believe that this is our page. If you look at the people who liked this page, some of them are the supporters of the real [organization]."

"So, this happens all the time. There's a Facebook page... that copied my logo. It's not a parody, because they do attack. They will share anti-feminism news on Facebook, and tag our page... or share abortion or rape memes and tag our pages."

In the above quote, the interviewee identifies that impersonation is harmful and not humorous or lighthearted as could be indicated by the term 'parody', in which accounts are created to satirize people or organizations. These accounts are deliberately misleading, create confusion, compromise the legitimacy of organizations' messages, create reputational damage and even harm or threaten. One interviewee suggested that it was "not a coincidence" that these pages became more numerous and increased the intensity of their activities when there were political or contextual issues concerning gender and human rights in the media. These were organized and deliberate campaigns of misinformation and disinformation against feminist and gender rights advocating groups.

3.2.2 PERSONAL CYBER THREATS

Respondents were also asked whether they had personally experienced a variety of threatening actions online. These have been mapped to the broad threats highlighted in the previous sections (see Table 4).

In accord with the results concerning organizations, phishing and having a virus on one's device were some of the most commonly experienced personal cyber threats. Other widespread experiences were being threatened, being exposed to unwanted explicit content, one's device being hacked and information being shared without consent. To explore these experiences in more detail, the experiences of participants as a function of their gender and whether they were employed in a WCSO as compared to a CSO were examined.

Results show that there are many similarities by gender, and where there were differences, these were not in the direction that would be expected by the research. For example, a higher proportion of men reported rumours, information and images (intimate and non-intimate) were distributed about them online. In contrast, a greater proportion of women indicated that they had been threatened online, bullied, stalked and received unwanted explicit material. Although the differences are relatively small, they are notable in that they illustrate the different types of threats reported by men as compared to women in this sample; specifically, a higher proportion of men reported breaches of privacy online, whereas a higher proportion of women experience threats and violence (both sexual and otherwise). These results may indicate that men working in civil society experience different types of online issues than women, but it is unclear whether they experience greater than average online violence than men who do not work in civil society. The results for women replicate the broader literature concerning technology-facilitated gender-based violence, defined as "action by one or more people that harms others based on their sexual or gender identity or by enforcing harmful gender norms. This action is carried out using the Internet and/or mobile technology and includes stalking, bullying, sex-based harassment, defamation, hate speech, exploitation and gendertrolling."[48] Research has found that this type of online violence is prevalent in the region and has widespread negative social, economic, and health consequences of those affected and on the organizations and communities where this occurs.[49]

There were also distinct differences in personal experiences of cyber threats for those who are employed by WCSOs as compared to CSOs. **In general, those in WCSOs were more likely to have ever personally experienced at least one or more of the cyber threats presented. The largest difference concerned the incident "false information has been spread about me," with nearly half of individuals employed in WSOs having had this experience as compared to 19 per cent of those employed in CSOs**. There were also noticeable differences in the proportion of those who had been stalked, trolled, had rumours spread or had been impersonated, all of which are oriented towards targeted types of attacks to undermine or misrepresent. While caution should be taken in this interpretation given the differences in sample sizes of the groups, this may indicate a pattern of targeting by external actors.

48 Hinson, L., Mueller, J., O'Brien-Milne, L., & Wandera, N. (2018). Technology-facilitated gender based violence: What is it and how do we measure it? Washington: International Centre for Research on Women. https://www.icrw.org/publications/technology-facilitated-gender-based-violence-what-is-it-and-how-do-we-measure-it/

49 USAID. (2022). Landscape Analysis of Technology-Facilitated Gender-Based Violence: Findings from the Asia Region. https://pdf.usaid.gov/pdf_docs/PA00Z7GS.pdf

TABLE 4. PREVALENCE OF PERSONAL EXPERIENCES OF CYBER THREATS

TYPE OF PERSONAL THREAT	DETAILED ASSESSMENT OF PERSONAL THREAT	MEN[50]	WOMEN AND GENDER DIVERSE PERSONS[51]	CSO[52]	WCSO[53]
Data breaches	My personal information has been shared in a data breach	42%	**43%**	42%	**41%**
	Non-intimate images or videos of me have been shared online without my consent	42%	**28%**	38%	**31%**
	Intimate images, videos or of me have been shared online without my consent	29%	**9%**	14%	**16%**
Disinformation	False information has been spread about me over digital media	54%	**33%**	19%	**47%**
	Deep-fake images or videos of me have been made and shared online	25%	**15%**	19%	**18%**
	Others have pretended to be me online	33%	**35%**	24%	**37%**
Doxxing	My personal information has been shared online without my consent	54%	**52%**	52%	**53%**
Hacking	My account or digital device has been hacked	54%	**53%**	45%	**55%**
Online harassment	I have been threatened by others online	42%	**54%**	52%	**49%**
	I have experienced online bullying	37%	**46%**	43%	**41%**
	Rumours about me have been shared online	42%	**17%**	13%	**29%**

50 In the survey, 27 respondents identified as men.
51 In the survey, 51 respondents identified as either women (42) or non-binary or as having another gender (9)
52 n = 24
53 n = 56

TYPE OF PERSONAL THREAT	DETAILED ASSESSMENT OF PERSONAL THREAT	MEN[50]	WOMEN AND GENDER DIVERSE PERSONS[51]	CSO[52]	WCSO[53]
Online harassment	I have been subject to sexist or discriminatory hate speech	21%	**29%**	35%	**24%**
	I have received unwanted intimate pictures, videos or messages online	46%	**54%**	48%	**55%**
	I have been stalked online	37%	**46%**	33%	**49%**
Phishing	I have received emails or messages designed to trick me into falling for a scam	92%	**93%**	90%	**94%**
Ransomware	I have been subject to a ransomware attack	17%	**9%**	14%	**12%**
Spyware	I have had spyware or software designed to gather data about me on one of my digital devices	42%	**30%**	33%	**35%**
Trolling	I have been trolled	42%	**30%**	33%	**49%**
Viruses	I have had a virus on one of my digital devices	71%	**78%**	65%	**80%**
Other threats	My family members were targeted online to try to harm me	21%	**13%**	19%	**14%**

*Percentages indicate the proportion who had ever experienced the cyber threat listed

The prevalence of cyber threats directed at individuals was reiterated in the interviews. The stories shared were wide-ranging, including personal experiences, but also drawing on the stories of known others. The harms caused by cyber incidents were often discussed directly. For example, a common experience discussed was the hacking of a website or social media, with resulting data and financial losses as well as loss of trust and feelings of security:

"There was a hack on my colleague's Telegram, and that's why I feel a bit insecure for myself as well because I do a lot of communication through Telegram and a lot of sensitive information is out there."

"My colleague is an outspoken women rights activist... they are often being hacked through [social media]. Texts were sent by somebody else using her account, people thought it was sent by her, but it was sent by someone else... And it's very dangerous...particularly for us as women's rights defenders."

Hacking can have long-lasting and devastating impacts, as alluded to in the above quote where this was labelled as "dangerous," especially when coupled with identity theft:

"I've had my Facebook site hacked. I haven't personally had my identity changed, but I have friends who have had their identity stolen online, and it's been an excruciating process to try and reclaim that."

The "excruciating process" of recovering from identity theft in the form of emotional and physical symptoms of distress has been corroborated in the literature.[54] A critical insight was that **hacking and fraud on social media reduced agency and empowerment because individuals use these platforms to express themselves and connect with others**. Notably, it was suggested that social media assisted in supporting 'digital citizenship', which is a critical part of identity for WHRDs. Not being able to engage in this negatively affected freedom of expression, and, as a flow-on effect, negatively impacted feelings of fulfilment and meaning in advocacy activities. It was also noted that this was likely to be a common occurrence due to the high degree of cybercrime in the region, with one respondent highlighting that this was part of a growing criminal industry:

"Hacking of accounts and digital identity theft has proliferated [in our country] ... the generation of fake accounts to use for cyberbullying, cyberattacking people ... social media hacking and digital financial fraud — they are all part of a big industry [here] there's even a troll farm."

The content and type of personal threats experienced by WHRDs often took the form of sexual harassment. For example, several interviewees discussed how threat actors targeted their attacks at women protesters, calling them (and the way they dress) both "sexy" and "obscene." In one instance, information about protestors was found (or fabricated), and in another, explicit photos were taken and these real and fake intimate images were sold and/or shared online without consent. The distribution of these images was then used as a means to imply that women protestors were sexual objects to be "seen" at these events or that they were sex workers.

"Another violent form is photo taking and selling them on [social media]. Sexy photos, photos taken from under the skirt, suggesting that if you come to the assembly you will see these cute women."

"As we campaign for bodily integrity, some people dressed up in styles that look sexy or went nude. Then [perpetrators] used the photos and mentioned we don't have good morals or suggested that if you want to buy [sexual] services, you can buy them from us. Which is very serious sexual harassment."

Effectively, the perpetrators moralized, sexualized and degraded the protestors, all of which devalued the movement. As one interviewee noted, these strategies made the aims and demands of women protestors "become invisible or get overlooked" and that the information spread about women acted to "dehumanize" them.

This type of intentional undermining was evident in other narratives of attempts to discredit groups and individuals or to create confusion through deliberate public campaigns of misinformation, trolling and hate speech. Such experiences were described as taking a major toll on the mental and physical health of individuals as "it makes the assembly space unsafe," causing stress and anxiety, that "they are tired, they want to quit," and prolonged issues that had little recourse or solutions for victims who were often retraumatized:

"Staff do suffer from this, of course. They have to read these negative comments all the time. There was some time that our staff could not hold themselves back and they posted a reply back. Then their Facebook profile became a target... mentally that staff member felt so bad."

"She got more than a thousand comments... this was too much for her. That's why during that time she had to stop using the Internet and had to meet a doctor."

"When it comes to sexual harassment, we have to be very careful...because we don't want to push this case into the spotlight. If the sex tape or sexual clip has already leaked on the Internet... how can we make the public help? And how do we handle the emotional breakdown, the anxiety, the harm of the thing? But we don't normally pay attention to the mental health issues related to cybersecurity."

Another notable concern with these types of personal cyberattacks is when they intersect with offline space, especially regarding interactions related to cyber-stalking, surveillance and privacy breaches. The following quote highlights a specific case where these issues intersect:

"My friend, who was in a crowded space, bumped into a man who swapped phones with her and was then able to track her movements."

Although this situation was not a common occurrence, the quote highlights how technology can put victims

54 Golladay, K., & Holtfreter, K. (2017). The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes. *Victims and Offenders, 12*(5), 741–760. https://doi.org/10.1080/15564886.2016.1177766

at risk for harm beyond those experienced online. Interviewees related concerns over surveillance and location tracking a variety of times. Notably, participants mentioned being very careful about not sharing their location (especially real-time sharing), not tagging their locations in posts, not posting photos where their location could be deduced, and even entirely turning off GPS location on their devices.

In most instances, participants were more concerned about surveillance by organized threat actors than tracking by individuals. Some WHRDs, especially those in leadership positions, felt that being the target of personal cyber threats was something to be expected — but certainly unwarranted and damaging — due to the high-profile nature of the work that they engaged in. This resulted in cultivating a sense of vigilance, where individuals worked to protect themselves and prevent, wherever they could, incidents from happening.

"Personally, I feel that it is expected ... I was very, very careful not to allow myself to be harassed by these kinds of people. I know that it might come to me, and I know that if it comes to me, this is the level that it could be. But I cannot let it go beyond this level; if it does, then I might have to take some action. So I had it in my mind made up already. I used to say [my thoughts and feelings online very openly] but I stopped doing that after I shifted to my current position."

The above quote, from a well-established leader of a women's rights organization, **highlights the experience of needing to negotiate 'expected' and unavoidable levels of online violence and harassment**. For the interviewee, what was an acceptable versus unacceptable level of personal cyber threats was very much shaped by the understanding that those who advocate for women or within a feminist context are likely to be critical targets.

3.2.3 GENDERED CYBER THREATS FOR WCSOs AND WHRDs

To examine issues of gendered risk in more detail, participants were asked whether they believed those who work with or advocate for women and girls are at a greater risk of cyber threats and why. A large majority said that they did believe that this focus puts individuals and organizations at risk. Some mentioned the evidence for this in the sexism, gender-related hate speech and trolling they received.

"Yes. Often we received sexist comments or trolling for work we are advocating for gender rights."

"Yes, women and girls are targeted by threats such as violence or abuse online."

Others mentioned the stereotypes or norms around gender as a reason:

"Yes, women and girls are at a greater risk because they are already more vulnerable in the first place."

"Yes, they are more prone to get attacks because attackers think women are lacking the skills and knowledge to protect their devices."

As the following quotes illustrate, the targeting of women advocates mirrors offline inequalities and power relations:

"Yes, advocates of women's rights are at greater risk of cyberattacks because of the macho patriarchal culture where women are treated as lesser than men, regardless of their socioeconomic class, which makes other people more confident in threatening these women. Even outside of their political work, female activists get harassed just because they are female."

"Yes, because the general culture that promotes the views that can be considered as patriarchal and macho continue to persist, and gendered attacks, which largely include various forms of sexism and sexual violence, are being done and promoted by government actors."

Additionally, several comments indicated that the targeting of WCSOs and WHRDs was a likely outcome of the nature of gender equality issues more broadly, which are often in the public eye.

"Yes. Especially now that our country has an anti-terrorism law, [this] red-flags individuals and groups that are critical to state's anti-people, misogyny and other human rights violations."

"The CSOs who advocate not for women and girls but for gender equality (of all genders) shall be at risk of cyberattack to some extent. Particularly for those who promote women's rights, which is a high-profile issue."

Some participants, however, did not believe that WCSOs and WHRDs were specifically targeted due to issues relating to gender, but rather some were opportunistic and economically motivated attacks; *"[mainly] it is scammers asking for money or something like that,"* and others were due to the nature of advocacy and activism. Some mentioned that rather than cyber threats being centred on gendered issues, WCSOs and WHRDs that

worked on politically sensitive topics were targets of cyberattacks; WCSOs and WHRDs were targeted because gender and women's rights issues are often considered as contentious in the Southeast Asian region (or "high-profile" as mentioned in the quote above). As highlighted by one of the interviewees:

"All organizations have cybersecurity concerns in this complex context. Every organization may have cyberattacks at any time, depending on its thematic targets. I feel that the greater risk of cyberattacks more depends on thematic focus ... in this politically high-risk period."

As indicated by the above quote, in less politically, economically and socially stable contexts, cyber threats could be seen as a lever to disrupt advocacy and activism in a deliberate, thematically driven way. Furthermore, when assessing the reasons why specific organizations or individuals might be targeted by threat actors, it was suggested that researchers look into who gains from the potential harms caused or whoever benefits the most from undermining operations.

It was also noted that cyberattacks that were not targeted at WCSOs and WHRDs often had gendered effects, especially in conflict-affected nations. Because women are the main clients of support services in areas of conflict, when CSOs (regardless of their mandate) experienced adverse cyber events, women typically experience more negative impacts from disruption of services than men.

In general, the topics of gender, human rights, and political instability were understood to be intertwined and complex issues in the region whereby cyberattacks are used to suppress the voices of women and to undermine feminist discourse:

"More women, of course, are victims [of gendered harms]; they are being targeted. Whether it's online surveillance or whether it's hate speech — hurling obscene, abusive words and statements against us. So we feel that burning hate against women, just because they are women... and when you say something critical of the government, and then they target you [more severely]."

The suppression of feminist discourse was also mentioned as directly related to social media. One such example is the use of the term *'femtwit'* (a portmanteau of feminist and Twitter). This was developed as a derogatory label for digital activists with a feminist agenda who gathered support for their cause through Twitter. Anti-feminist movements created and used this term to undermine the efforts of online activism, creating an image of bad, ineffectual or lazy feminism.

"The anti-feminism group tried to label us as 'bad feminists'. So, they suggested that 'femtwit' should go to the protest or do something real, not on Twitter, not just talk on Twitter. And that is the attempt to separate femtwit from feminist."

These efforts to diminish the online work of WHRDs may seem to be relatively minor and could even be argued to support some other types of feminism (e.g. those that are carried out in person). In reality, however, these were sophisticated attempts to discredit WHRDs and had major consequences because the term was used as a tool to mobilize groups to engage in violence against women.

"Some accounts said if they see femtwits, they will beat them. Or some of them say that they will kill femtwits ... kill them, beat them. It spread out on Twitter, and one day, I saw this kind of hate speech, so I took a screenshot of that Twitter account, and I tweeted about that thing saying that this is femicide because you want to kill feminists."

Even in situations where there were threats of death or injury, WHRDs had very little recourse to protect themselves due to the perceived lack of seriousness of online threats. Notably, some WHRDs hold the view that what happens online should not be considered as a "real" threat:

"Even when we talk with human rights defenders in [my country] about this kind of violence, they said it's not violence. When I talked with [a WHRD], I said that group did something bad to us, she said that this is just trolling and the men in that group cannot do anything in real life."

In this context, online harassment was considered to be unrelated to offline violence and to be treated as less serious or impactful than in-person threats. These attitudes were also reflected in national-level policies that were discussed as often offering little to no protection for individuals:

"We talked a lot about what we can do about this kind of digital threat because in each country in Southeast Asia, there is no law to protect us from digital threats. We have the Computer-related Crime Act, but it never protects us from this kind of thing. They've never protected us from people who harassed us or made hate speech against us."

Under these conditions, two critical, interrelated outcomes were highlighted: withdrawal from advocacy and activism and issues with mental health.

"So, it happened with Muslim women and also feminists [they quit]. Many other accounts also had to be deactivated because they got a lot of sexual harassment, they got a lot of like bullying online."

The result of gendered cyber threats, ongoing sexual harassment, bombardment from multiple threat actors, lack of formal and informal protections and the associated feelings of stress, ill-health, and helplessness that followed these incidents is illustrated by the following quote as the "real violence":

"[A WHRD] also had to shut down herself from interviews, from speaking out, or posting her photos. This is an effect of gender trolling, **and I think this is another violence, right, this is another kind of violence that we don't recognize. This is real violence for us. We feel unsafe to speak out**."

"This is not only about the mental effects; **it's about how this silences the space for us as well**."

3.3 Cyber Vulnerabilities

In the context of cybersecurity, vulnerabilities refer to technical or non-technical weaknesses that provide opportunities for exploitation by threat actors. Technical vulnerabilities include flaws in digital infrastructure such as operating systems exploits, unsecured networks, outdated or unpatched software and lack of robust data encryption. Non-technical vulnerabilities refer to human or social factors that arise from policies, procedures and user behaviours rather than issues in the technology itself. For example, weak passwords, poor technological or physical security awareness, low levels of digital literacy, and psychological or emotional characteristics (such as distraction, greed, bias or even empathy) that threat actors can manipulate to achieve their goals.

CSOs often have unique and intersecting technical and non-technical vulnerabilities due to their aims, funding and staffing. For example, CSOs may have limited resources to invest in cybersecurity measures or may not have dedicated technical staff to manage their digital security. WCSOs are often staffed by women, and these women are subject to gender stereotypes whereby they are less likely to have experiences that support and encourage digital efficacy and literacies. The following sections highlight some of the critical vulnerabilities that WCSOs and WHRDs face.

3.3.1 TECHNICAL VULNERABILITIES

Those who are not ICT professionals may find it challenging to identify technical vulnerabilities given that they are unlikely to have access to their organization's technical operations, digital networks and systems. As system users, however, participants were aware of some critical vulnerabilities with digital technologies. For example, the previously mentioned utilization of devices for both work and home and the potential for information leaks via social media were understood to be vulnerabilities. Participants mentioned the culture of "BYOD" ("bring your own device") and the changes in practice from working in offices to home-based or public working environments as a result of the post-pandemic "new normal" as exacerbating these issues.

The protection of devices, particularly those that spanned personal and professional use (typically laptops and phones), was also recognized as a weakness because most participants did not utilize protective functions such as authentication measures or automatic screen locking. Additionally, the use of unlicensed software (and therefore less likely to be eligible for updates or patches) was widespread, especially among organizations that were less well-resourced. This intersection between technical vulnerabilities and resourcing is very important to note; an interviewee described the complexity of these issues:

"Most of the small groups are still using the antiquated systems, which are easily hacked or attacked ... the first thing you have to have is an inventory of which particular devices we are using for our work. Then we have to think about how to make our devices secure ... and how do we understand the security condition of the devices or check if our system is under threat or not? Because that's the problem, even if we buy a lot of new things (devices or systems), if we do not check them regularly, they are not updated and then perhaps we are not solving the problem of cybersecurity at all."

Resolving technical vulnerabilities is not a straightforward issue of upgrading devices or systems, but rather requires a wraparound strategy for continuous implementation of cybersecurity measures. Therefore, funding new assets to resolve technical vulnerabilities is likely ineffective and may make matters worse by appearing to have removed a weakness but without taking into account the sustainability of the solution.

Many participants mentioned a range of technical solutions to protect against known threats that their organizations already implemented, including various forms of multi-factor authentication (MFA), locking

down access to files and folders on cloud-based storage, organizational and personal use of VPNs on computers and mobile devices, and not displaying email addresses or personal information on public websites.

Overall, technical vulnerabilities were discussed substantially less than organizational, social and human factors. This should not be interpreted as though technical vulnerabilities are unimportant, but rather that they may be difficult to articulate and address for those who are not ICT experts. This issue was specifically mentioned by interviewees, many of whom did not have technical roles in their organizations;

"I acknowledge that the staff whose work is not tech-related creates a lot of the risk. Not the tech specialists."

"There is a problem with the user more than the infrastructure. Human error is a huge issue for us ... a reason is that they don't know. So the vulnerability starts with the people, and the technology keeps increasing"

Several interview participants who were in technically oriented roles within their organizations strongly reiterated this sentiment:

"Having a strong tech background, we have stronger mechanisms compared to our partners."

"Well, compared to other organizations ... a majority of our staff are in tech, so I assume we could more easily rely on them on how to address [technical cyber vulnerabilities]."

However, as aptly illustrated by the following quote (from a professional digital security trainer), training for the technical elements of cybersecurity was often ineffectual and could even be misguided due to the more difficult parts of cybersecurity to change, i.e. staff behaviours and habits.

"When we have cybersecurity training, most of the content is about the technical; it's about IT, about the jargon terms, about applications. But what we found out is that the challenging issue is not technical, but it's about behaviours and habits... changing these is more challenging."

3.3.2 CYBERSECURITY POLICIES AND PROCEDURES

The following sections explore organizational policies and procedures concerning cyber security and staff perceptions concerning the efficacy of cybersecurity management strategies.

FIGURE 7. WCSOs' ORGANIZATIONAL CYBERSECURITY POLICIES AND PROCEDURES

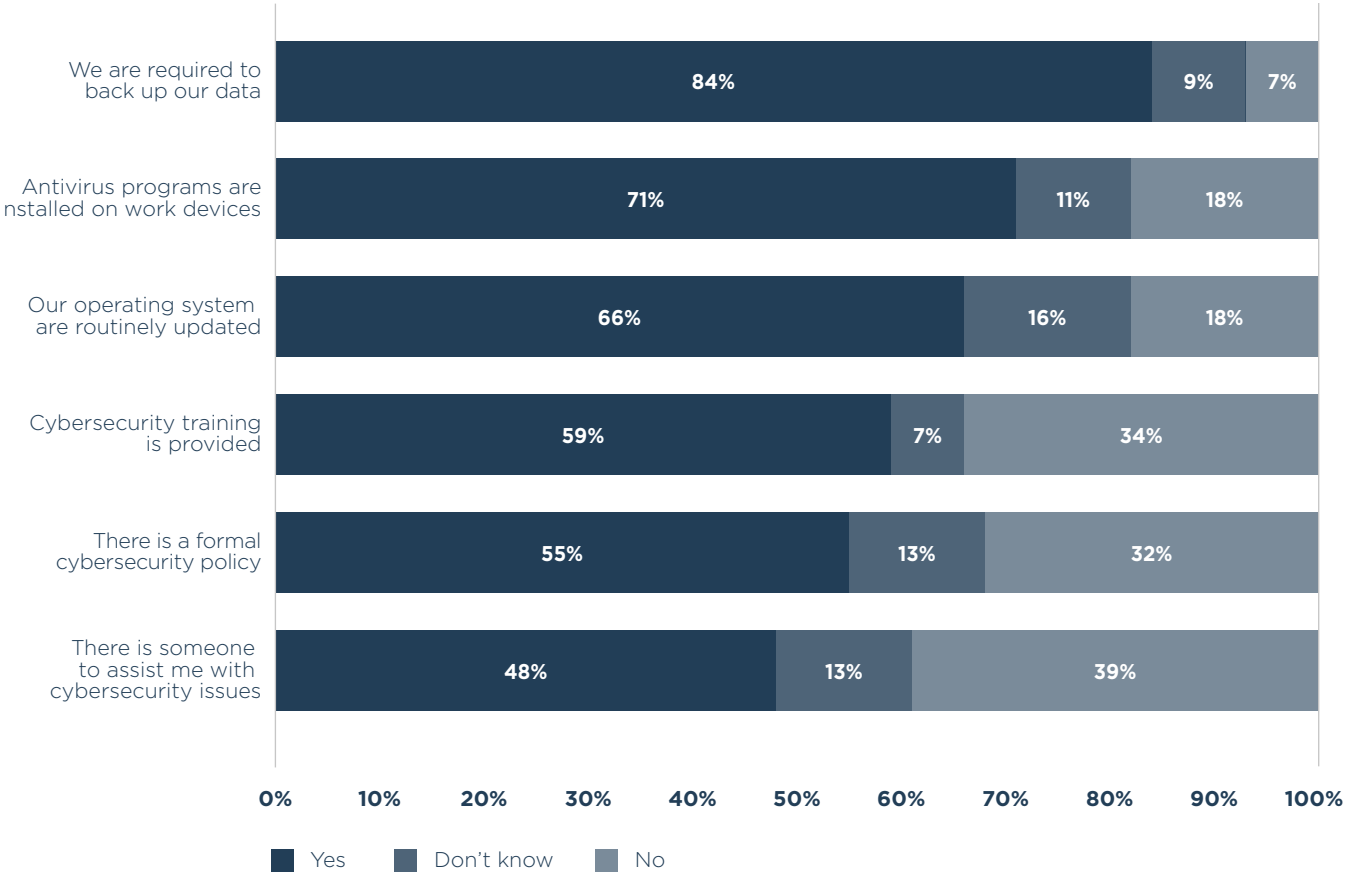
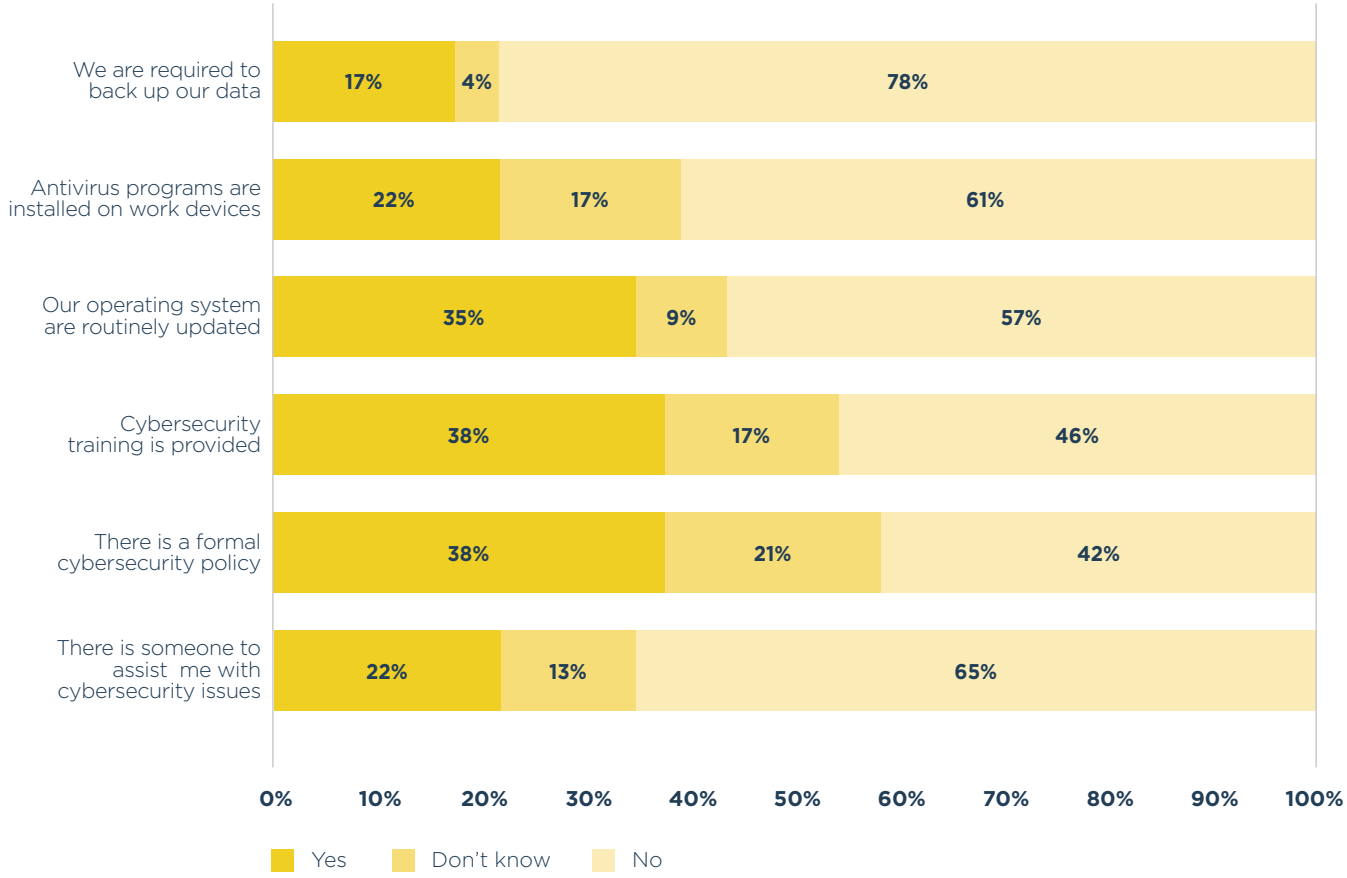


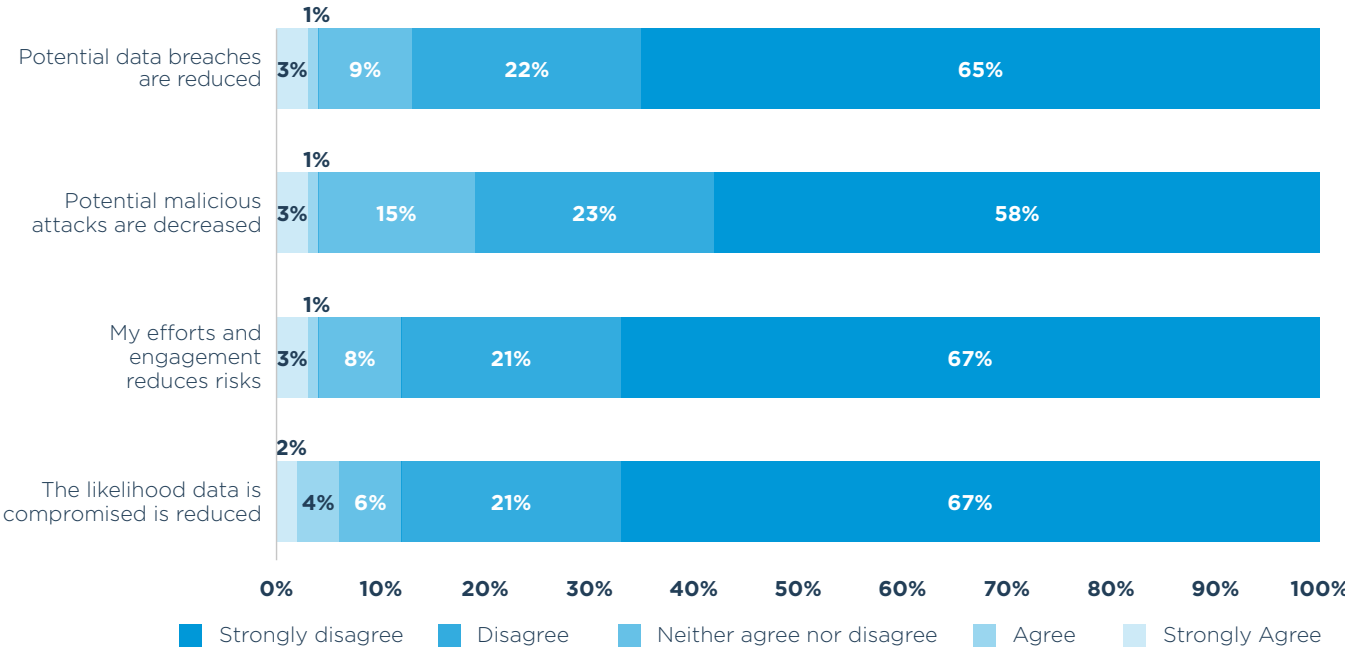
FIGURE 8. CSOS' ORGANIZATIONAL CYBERSECURITY POLICIES AND PROCEDURES



Figures 7 and 8 illustrate the proportion of WCSOs and CSOs where there were processes in place to address cybersecurity. Overall, WCSOs were more likely than CSOs to have the listed policies and procedures in place. For example, over half of WCSOs said that their organizations had a formal cybersecurity policy (55 per cent) and that they received training on cybersecurity (59 per cent) as compared to those in CSOs, were the proportions were 42 per cent and 46 per cent, respectively. Furthermore, over two-thirds of WCSOs had antivirus software and said that their systems were regularly updated, which was substantially higher than for CSOs. **Notably, however, WCSOs lagged behind by a large margin in terms of having a dedicated person in their organization who could help them if they had a cybersecurity issue — 48 per cent of WCSOs compared to 65 per cent of CSOs**. Also, between 3 per cent and 20 per cent of participants were not sure whether their organization had these factors in place. Additional results indicated that very few participants (n = 4) had none of these in place (or did not know), but there was a relatively large number (n=16) who had all of these in place. The protective factors that were more passive and potentially less resource-intensive were the most commonly implemented strategies. Overall, there was a high level of awareness and formal uptake of mechanisms that reduced technical cyber vulnerabilities. Finally, individuals were asked whether they believed that their actions in following cybersecurity policies and procedures would have efficacious outcomes. There were no major differences between WCSOs and CSOs; therefore, results were combined in Figure 9. A large majority of participants agreed or strongly agreed that adhering to processes was impactful. Specifically, following organizational policies was thought to reduce overall cyber risks and to be a strong protector against data breaches, cyberattacks and data compromise.

These results indicate that individuals believe that cybersecurity procedures at the organizational level are important and that their efforts to follow them have a protective function for the organization. Similar to the results regarding threat knowledge, this is an important finding to highlight because previous research argued that individuals do not follow through with cybersecurity procedures because they think they are unimportant or ineffective. This does not seem to be the case for this sample. Therefore, supporting secure cyber practices focusing on shifting negative attitudes is unlikely to be efficacious (as participants are already primed with high levels of knowledge and positive attitudes towards cybersecurity).

FIGURE 9. EFFICACY OF FOLLOWING CYBERSECURITY PROCESSES FOR WCSOS AND CSOS



Alongside the strong support for institutional cybersecurity policies and practices as found in the survey results, many interviewees also discussed adhering to a set of rules, regulations and norms within their organization around online protections. For example, several WHRDs worked in organizations where there were regular cyber hygiene trainings, some of which were informal and many of which (especially in the larger organizations) were mandated. These same organizations tended to have dedicated ICT support, high-level technology strategies and technical rules and regulations in place (e.g. multi-factor authentication and policies on data privacy and storage). WHRDs who work independently or in smaller, localized organizations described fewer of these protective elements in place due to resourcing issues. However, there was a strong appetite for additional support within these organizations and a high level of awareness of the importance of cybersecurity strategies (as subsequently discussed).

3.3.3 INFORMATION SECURITY BEHAVIOURS AND BELIEFS

While technical measures, such as antivirus software and encryption, can reduce cyber vulnerabilities and assist in protecting against cyber threats, it is well established that these measures are not sufficient on their own. One of the key reasons for this is that the way users engage with technology, and whether or not they are both aware of and choose to engage in secure cyber practices, is contingent on several psychological and behavioural factors. These factors are broadly captured in the research concerning information security behaviours and beliefs.

For example, it is often up to individuals as to whether they use strong passwords (as well as keep this secret and not use the same passwords across applications). Individuals may also be responsible for actions such as applying software updates and the safe or encrypted storage of sensitive data. Additionally, users are responsible for their choice of whether to click on potentially harmful links, lock their devices or make sure others cannot view or access devices when in public. Furthermore, beliefs concerning the importance of secure cyber practices, the choices made to adhere to policies and procedures and the awareness of security best practices are all very individualized, important, non-technical cyber vulnerabilities.

We asked participants about their information security practices that potentially undermine their cybersecurity and about those practices that are protective (see Figures 10 and 11). The results indicate that the majority of participants do not engage in poor information security practices, with strong disagreement regarding insecure practices (items 1 – 5) and strong agreement regarding secure practices (items 6 – 12).

Regarding non-secure behaviours, individuals were very unlikely to click on links, open attachments from unknown senders or leave devices unattended, which are the most common mechanisms for phishing and related risks of malware or data theft. However, individuals in WCSOs were more likely than those working in CSOs to strongly agree or agree that they **post whatever they want to on social media**, specifically 28 per cent of WCSOs, as compared to 10 per cent of CSOs, agreed

FIGURE 10. WCSOS' INFORMATION SECURITY BEHAVIOURS

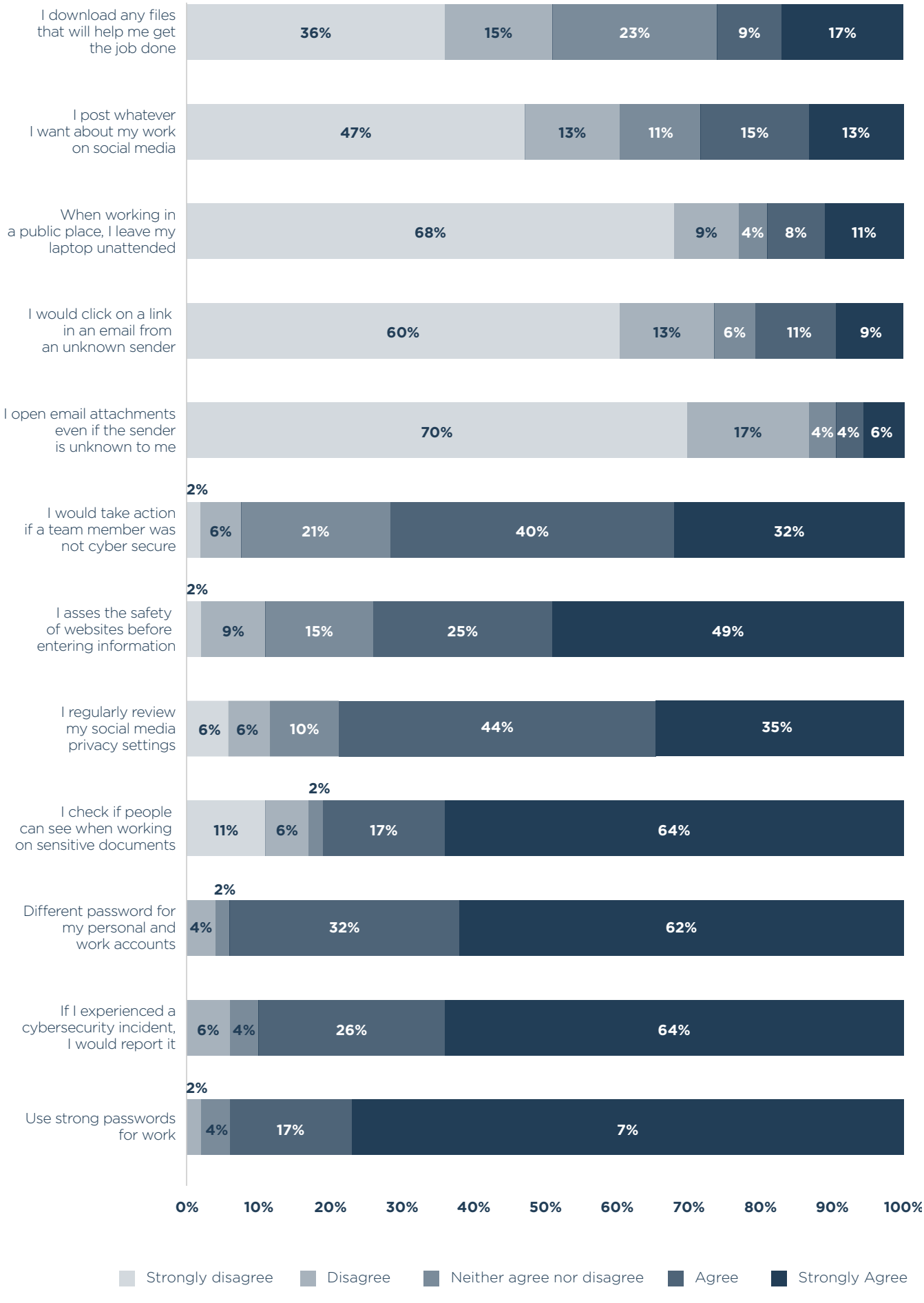
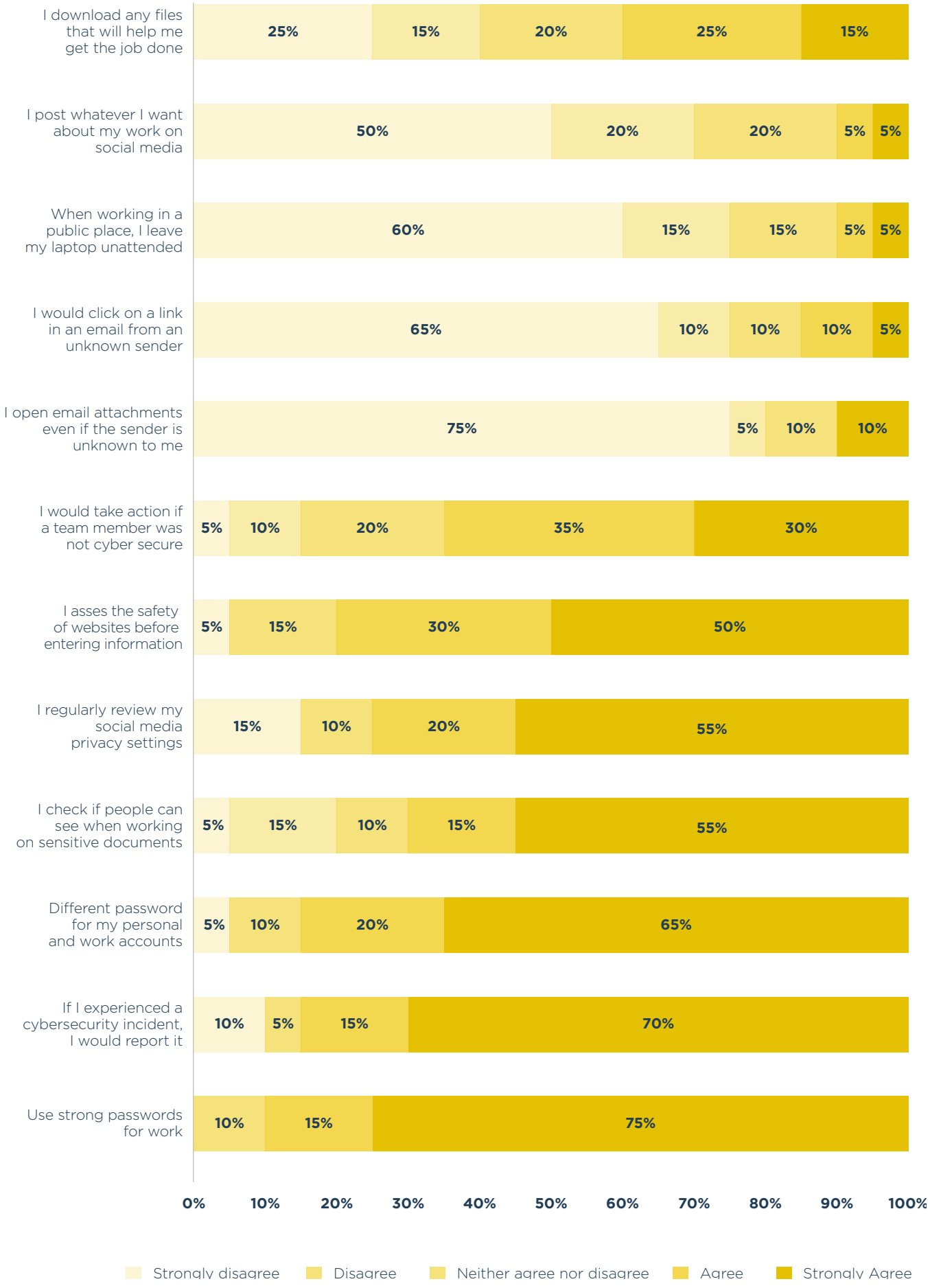


FIGURE 11. CSOS' INFORMATION SECURITY BEHAVIOURS



with this statement. Also, a large proportion of participants agreed that they would **download any files onto their computer that would help them get work done**, although the pattern was reversed with more CSOs agreeing to this statement compared to WCSOs (40 per cent versus 26 per cent).

These findings are concerning, but not unexpected, particularly in light of the previous results showing that WCSOs often rely on their personal devices and social media accounts to undertake their work. Also, intentional posting on social media is an important and functional part of WCSO work; they already have to manage the related risks. Therefore, this result may have less to do with non-secure practices and more to do with the logistical constraints of the work environment.

Additionally, it is well known that many CSOs rely on freely available software and applications for their work (either open-sourced or unauthorized) given resource and financing constraints, so the propensity to download files to assist in work is not uncommon. Interviewees mentioned that this was due to the high costs of purchasing licensed software and subscriptions, especially those in small organizations or individual WHRDs. Although obtaining software this way may be a practical solution, it introduces vulnerabilities for WCSOs and WHRDs and heightens the threats of viruses and malware (through illegal downloads, the software itself, or the lack of ability to patch or update).

Participants were also asked about their behaviours that support and are protective of personal and organizational cybersecurity. As per the results above, the large majority use strong passwords (these were defined as those with sufficient length and that use numerals, lowercase and uppercase characters and symbols), kept separate passwords for work and personal accounts, and made sure to keep their devices secure in public.

Notably, however, fewer individuals actively checked the safety of the websites that they accessed or reviewed social media privacy settings. One of the reasons for this may be that these behaviours require active, near-constant engagement and vigilance, and, therefore, can be burdensome or difficult. However, it is recognized that checking websites for security and legitimacy reduces vulnerability to threats such as cyberstalking, identity theft and malware.

Maybe even more importantly, given the widespread use and importance of social media for WCSOs and WHRDs, is checking the privacy settings on these applications. Many default settings leave users open and vulnerable to cyber threats, and even if individuals are active, long-term users of social media, these platforms often update their policies and settings.

Finally, respondents were asked whether or not they would report a personal experience of a cybersecurity incident or if they would take action if they saw a team member engaging in non-secure practices. The results illustrate that the majority (WCSOs = 88 per cent, CSOs = 85 per cent) would report a personal experience, although fewer (WCSOs = 72 per cent, CSOs = 65 per cent) would take action on behalf of a team member. This is an important finding, as research has shown that cybersecurity norms are a strong predictor of best practices within organization.[55] Specifically, better overall cybersecurity practices strongly correlate with socially agreed upon and accepted ways of responding to cyber risks that are modelled and reinforced by the group and maintained in the context of formal or informal policies and procedures

3.3.4 DIGITAL SELF-EFFICACY

Digital self-efficacy refers to an individual's belief in their ability to effectively and safely use, understand and manage digital technologies.[56] In the context of cybersecurity, digital self-efficacy is essential because it influences behavioural intentions as well as actual behaviours. Further, it has been found to have a strong positive relationship with cybersecurity compliance and information security awareness.[57]

Results (see Table 5) are collapsed across WCSOs and CSOs, as there were few notable differences. The findings show that respondents indicated high levels of digital self-efficacy overall, meaning that they felt confident in using technologies in a variety of ways. The most strongly endorsed items concerned efficacy in finding and sharing information (72 per cent agreement), which was closely followed by protecting one's own digital devices and by collaborating and positively interacting

55 Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*, 26-44

56 Ulfert-Blank, A. S., & Schmidt, I. (2022). Assessing digital self-efficacy: Review and scale development. *Computers and Education, 191*, 104626. https://doi.org/10.1016/j.compedu.2022.104626

57 Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly: Management Information Systems, 34*(SPEC. ISSUE 3), 523–548. https://doi.org/10.2307/25750690

with others. Notably, however, only 45 per cent of participants felt confident in their abilities to manage their digital footprint, and just over half felt able to solve technical issues that they might experience in using digital technologies. Additionally, many participants did not feel confident understanding gender-specific risks in digital contexts.

These results are encouraging, as research has broadly found that marginalized and vulnerable populations often feel low levels of ICT-related efficacy because of masculine stereotypes and social norms around expertise in digital technologies. It is important to note that the measure utilized in this research was able to identify distinct areas of efficacy related to digital technologies, including literacies, communication and safety. Indeed, the two items that were specifically focused on the *technical* elements of digital life had the lowest levels of endorsement.

These results highlight the importance of measuring confidence in utilizing technologies in a domain-specific fashion in order to attain a more nuanced understanding of efficacy and its relationship to cybersecurity. If we consider the research on ICT-related efficacy and information security awareness, it would be possible to conclude that women and minorities generally have low levels of efficacy in using digital technologies (due to systemic exclusion and discrimination). Furthermore, due to their low self-efficacy, it may be interpreted that they also have less secure cyber practices (as per the section above). Indeed, in this research, we found a strong, positive correlation between digital self-efficacy overall and information security practices ($r = .48$, $p < .01$). However, note that due to our focus on efficacy beyond the technical aspects, we were able to show that in the context of information literacy, effective communication and safety, this sample had overall high levels digital self-efficacy, which was associated with increased positive information security behaviours.

TABLE 5. DIGITAL SELF-EFFICACY

CONSTRUCT	DESCRIPTION	*HIGH EFFICACY	MEAN
Information and Data Literacy	Search for and find specific information in digital environments	72%	3.91
	Distinguish between accurate and inaccurate digital information	66%	3.78
	Store and organize digital content securely	62%	3.64
Problem Solving	Solve technical issues that arise when using digital systems	55%	3.48
	Identify and improve any digital skills I lack	68%	3.74
Communication and Collaboration	Share information and data with others digitally in a secure way	72%	3.83

* Proportion who "agree" or "strongly agree" that they feel confident in their abilities.

CONSTRUCT	DESCRIPTION	*HIGH EFFICACY	MEAN
Communication and Collaboration	Interact positively with others in digital environments	70%	3.83
	Participate safely in public discussions and activities in digital environments	67%	3.75
	Defend myself and others against injustice in digital environments	62%	3.71
	Use digital systems to collaborate with others	71%	3.87
Safety	Manage and delete my digital footprint	45%	3.17
	Protect my digital devices from unwanted access	71%	3.69
	Protect my personal data in digital environments	65%	3.65
	Protect the privacy of myself and others online	62%	3.64
Digital Social Awareness	Recognize the impact of digital environments in increasing social tensions	69%	3.78
	Recognize the gender-specific risks within digital environments	58%	3.56

4.

THE CYBER RESILIENCE OF WCSOS AND WHRDS

For this research, we define cyber resilience as "the ability of an actor to resist, respond and recover from cyber incidents to ensure the actor's operational continuity."[58] This conceptualization suggests that despite the probability of facing adverse cyber events, the associated risks can be mitigated in a variety of ways so that they do not have long-term negative effects — or may even have positive long-term effects (e.g. the ability to better manage future events).

Using the features of the definition as proxies for strategies to address adverse cyber events, the following section focuses on the ability of WCSOs and WHRDs to:

1. **Resist or prevent** — putting in place measures to reduce the likelihood of adverse events and the negative outcomes they may cause before the occurrence of an incident;
2. **Withstand or respond** — ensuring continuity and functionality of critical systems during and immediately after a cyber incident through timely and effective response mechanisms; and
3. **Recover or adapt** — restoring the systems and operations to their state before the adverse cyber incident and, based on the lessons from the event, improving or optimizing the systems or prevention and response mechanisms.

Following the three key features of cyber resilience, we asked survey respondents whether their organization was prepared, responsive and could easily recover from cyber threats. Preparation was strongly endorsed as an element of cyber resilience, with 53 per cent of WCSOs and 55 per cent of CSOs agreeing or strongly agreeing that their organization was "well prepared." The response was also rated high, even more so for WCSOs (55 per cent) as compared to CSOs (46 per cent) who agreed that their organization could respond immediately to cyber threats. Fewer (WCSOs = 45 per cent, CSOs = 41 per cent) agreed that their organization could easily recover from cyber threats, although this was still a relatively large proportion of participants. Therefore, overall perceptions of cyber resilience were generally quite high.

To broaden the exploration of these issues, a series of cases in which interviewees described different elements of cyber resilience are discussed below.

4.1 Resisting and Preventing Cyber and Offline Harms through Technology

The following case presents a brief account of how one organization used technology in novel ways to increase online and offline safety and security. Within the interviewee's organization, most active staff were volunteers who were recruited through open social media channels. This was an effective, but not very secure, method of mobilizing large numbers of people to their cause. It was noted, "at its peak, the open Telegram group had around 800 people. Inside

58 Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things, 11*, 100204.

that, there were volunteers, information operation, anything, we don't know." When referring to "information operation," the interviewee referenced deliberate campaigns to acquire information about the organization from non-legitimate supporters who joined the Telegram group. Given the openness of the group and the potential cyber threat actors, the organization intentionally segmented individuals into new groups for each event they engaged in, which were then deleted directly after the event. These subgroups were separated and had different levels of access, but came together in broader discussions where it was safe to do so. While this created additional complexity, it was also a mechanism to protect both information and people.

"Basically, there are walls in communication to ensure safety. Those walls that have been created are to protect the information in social media and information in our communications."

Another critical part of the organization's harm prevention strategy was a registration, check-in and check-out system that was connected to their in-person events. The system used online survey functionality for those who registered for events through social media to "check in" with a telephone phone number, but "without names or other personal information." Once participants returned home from the event safely, they would "check out" with the same link. Then volunteers would use this information to ensure that people who had attended events were accounted for, and if so: "our duty is then over, without the need to even know their names." This was particularly important because protesters and activists were regularly arrested, detained or targeted as a result of attending assemblies. Therefore, when a person did not check out after attendance, someone from the organization would personally contact them to ensure their safety.

4.2 Responding to Online Harassment

The next case presents an account of how WHRDs responded to coordinated cyberattacks via social media. The interviewee highlighted that the targets of attacks were leaders, board members and the spokesperson of their organization, who were all publicly associated with news stories related to the sensitive social and political issues that the organization advocated on behalf of. The interviewee mentioned that although they were very cautious and private in their personal social media use, this did not reduce the perpetration. One of the key mechanisms to manage this was using public reporting and blocking mechanisms:

"There were some posts that used my face or my name, and this goes against the community standards of Facebook. So I report when this happens a lot. It's not only me; anytime it happened to someone in our organization ... I actively used the Facebook report system ... it works. It works if you choose the right violation. But it has to be classified as a security issue or labelled as harassment for them to take action."

As highlighted in the quote, however, this only worked because the participant understood how to effectively use the reporting system and was able to report in a language understood by moderators, both crucial elements to ensuring that the violations were correctly coded so that they would be acted upon. Yet, for the same interviewee, the systems were not as effective for other types of harassment where there were many threat actors (or bots) acting in coordination to undermine or attack in other ways. This was especially the case where social media content was produced by others who tagged individuals or the organization and was open for comment.

"Comments will be like 'we hate you' ... and then the real fans, the real people, the real supporters, will feel intimidated and they don't want to engage in this conversation or want to type anything, or those who want to type something must be very courageous or must be very assertive to do so. That creates a very bad atmosphere for the page itself."

However, reporting functions could — and were — employed to respond to these issues. Indeed, this was one of the only mechanisms that could be used (because the organization relied on tagging to connect with its broader community, it could not simply disable the function). Yet it must be recognized that this was arduous, difficult, and resource-intensive for the organization, requiring ongoing vigilance and moderation.

"I try a lot to push the communications department to fix this. And one way to fix this is to mark the names and get all these accounts. First, if there was anything that crossed the line, we report. If one seems to be an inauthentic account, we also report that account to Facebook. And we did that, I think twice, so we have like the list of 100 to 200 of these people."

4.3 Recovering from a Data Breach

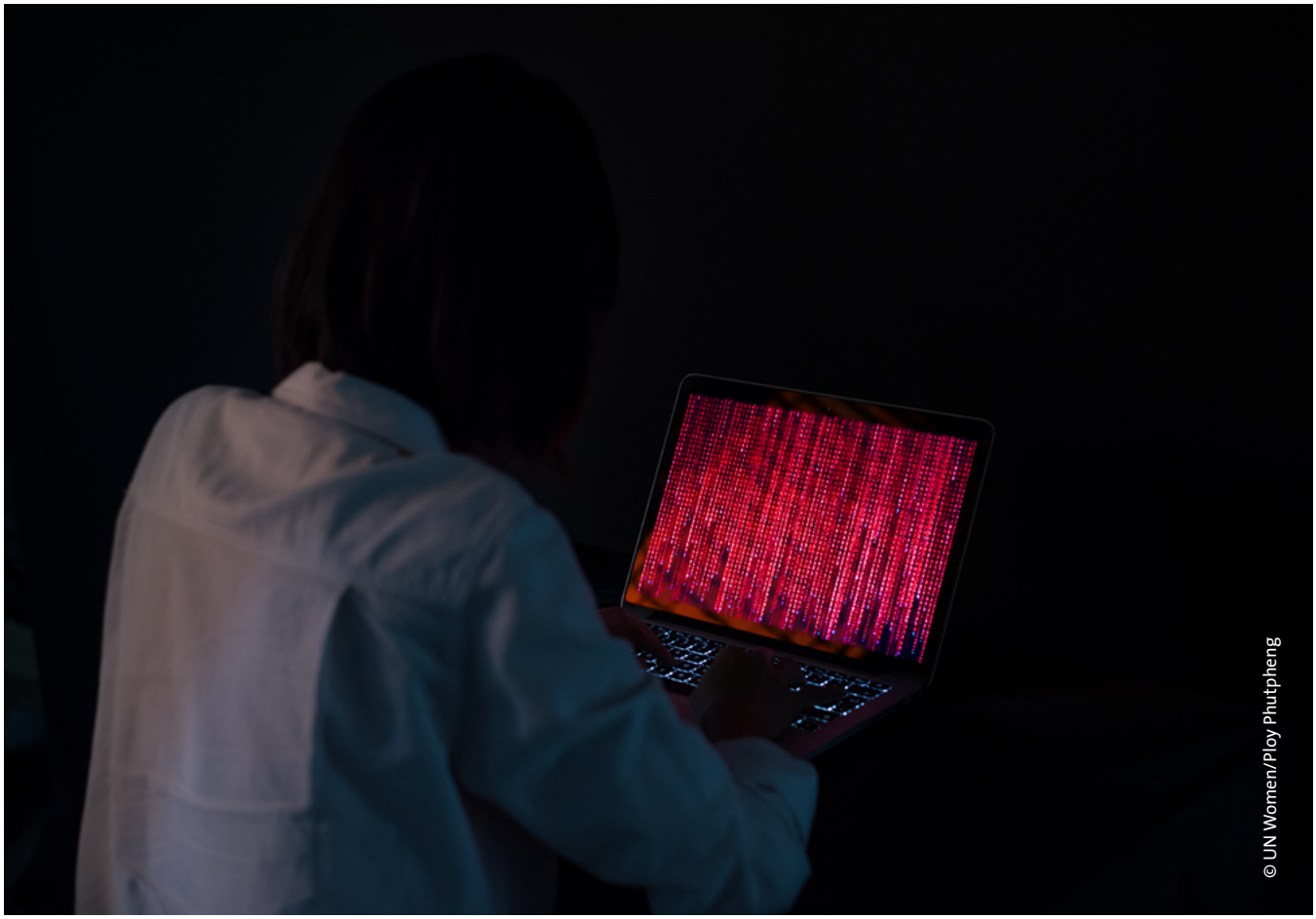
The final case presents an account of how an organization managed a leaked internal document and the ways it recovered from this event. The interviewee described the situation as one where sensitive information about their organization's campaigns and collaborations was shared by groups that were opposed to the organization's aims. The document had been distributed internally some months prior, and "the content itself was not dangerous at all," however, the sharing of this was alarming for broader reasons:

"That really scared us because we don't know how many of the documents were leaked, right. And because the one who got the document might wait until the right moment to use that against us ... the fact that it was leaked to outsiders, and this was used by [a malicious social media page] and some other conservative pages to [suggest that] he's trying to hijack or to disrupt [an event]."

Furthermore, it was difficult for the team to trace how the leak had happened because they were using password-protected and licensed cloud-based systems to host their documents and all other work-related information. After an investigation, it was found that the breach occurred once when a new work-related collaboration tool was used by a team that did not have sufficient technical protections in place and thus was exploited by threat actors.

In terms of recovery from this incident, the interviewee suggested that from a technical point of view, "it has not changed that much, because we didn't use that system before." However, from a cybersecurity awareness and implementation focus, the incident drew attention to poor and non-secure practices and helped the organization support messaging and change processes to ensure greater information security.

"Now, every time we access a document that is shared, we have verification. We cannot do many things, but we do this so leaks are not so likely."



Cybersecurity risks are a serious concern for WCSOs and WHRDs and their complexity needs to be addressed in multiple ways.

5.

CONCLUSION

The research results 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 reliance on technology can also expose individuals and organizations to cyber threats that may disrupt their work, damage their reputation and even create harm or injury. All of these impacts can further marginalize women's voices and participation in society and change-making processes.

It is clear that cybersecurity risks are a serious concern for WCSOs and WHRDs and that we need to address the complexity of these in multiple ways: through safer digital device practices, by actively protecting people and organizations from cyber threats and by reducing cyber vulnerabilities. **Critically, research findings indicate that there is a need for a strong shift away from techno-centric and generic approaches to human-centred and contextualized approaches to cyber resilience that centralize gender**.

While the challenges outlined in this report are widespread, they are particularly acute in politically volatile and conflict- and crisis-affected contexts, as highlighted by a number of respondents. The findings give depth to specific considerations for the conditions that need to be in place for WCSOs and WHRDs to safely sustain their work, which is a prerequisite for effectively implementing the WPS Agenda. Drawing from the Agenda's four conceptual pillars (participation, prevention, protection, and relief and recovery), key considerations that have emerged from the research are summarized below.

WCSOs and WHRDs face disproportionate risks of being exposed to cyberattacks and tend to have less access to resources that are needed to foster cyber resilience. This has negative impacts on their ability to safely conduct and sustain their work, which ultimately **restricts their operational spaces and ability to lead and participate in peace- and conflict-prevention efforts**. The lack of appropriate and context-specific resources, including access to learning opportunities, tools and financial means, results in higher levels of cybersecurity vulnerabilities and fewer opportunities to adopt strong prevention, protection and recovery efforts, which further compounds the aforementioned risks.

With online and offline harms being closely interlinked, WCSOs and WHRDs face significant risks of psychosocial and physical harm and, in some contexts, arbitrary arrest and judicial harassment. Due to a low degree of awareness of gendered cybersecurity considerations and a dearth of appropriate policies and response mechanisms to address the aforementioned risks, effective protection mechanisms and relief and recovery services for WCSOs and WHRDs are lacking, if not absent.

In line with existing evidence, the research findings highlight the lack of effective protections for WCSOs and WHRDs online. This further exacerbates the impact of cyber threats and attacks for said groups, and compounds the challenges of attaining appropriate and needs-based support. Moreover, while UN Member States have agreed in principle that international law should apply to cyberspace, there is still no consensus on how this should be done in practice. As a result, while cybersecurity laws and policies may be in place, WCSOs and WHRDs from some countries across the Asia-Pacific region raised the issue that these are not always purposeful and may, in certain cases, be used to limit civic engagement, freedom of speech and assembly and silence voices and agendas that may be perceived to be a threat to political status

quos. More efforts are needed to ensure that cybersecurity and policies are rights-based, context-specific and gender-responsive by ensuring that said frameworks are in line with international law, human rights conventions and WPS commitments.

As the WPS agenda is constantly evolving to respond to diverse security challenges, these factors must be further considered in policy-making and programming at the local, national and regional levels, as well as in the work of the United Nations Security Council and other UN bodies.

5.1 Key recommendations

Recommendation 1. Increase knowledge and awareness of gendered cybersecurity threats and vulnerabilities among civil society, governments, private-sector actors and other decision makers.

a. Engage in awareness raising campaigns to highlight the prevalence and impacts of cyberattacks on women's civic engagement and peace efforts. A focus on human-centric cybersecurity, the protection of human rights, and the minimisation of harms should be taken.

b. Document stories and lived experiences of WCSOs and WHRDs and their experiences related to gendered cybersecurity threats and vulnerabilities

c. 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.

d. 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.

e. 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.

f. Base the development and implementation of cybersecurity-related laws, policies and practices on international best practices and clauses outlined in international law[59], human rights conventions and WPS commitments.

g. 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.

59 While the International community has yet to find consensus on precisely how international law should apply to cyberspace, important strides have been made to set up a UN Framework of Responsible State Behaviour in Cyberspace, including by the UN Groups of Government Experts (UNGGE) and the Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security, as well as by the UNGGE on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. This includes the formulation of 11 voluntary and non-binding norms on responsible state behaviour in cyberspace, coupled with the recognition of the applicability of international law to cyberspace as well as calls for cyber capacity building and confidence-building measures.

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.

h. 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.

i. 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.

j. 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.

k. 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.

APPENDIX 1.

RESEARCH METHODOLOGY

A mixed-method approach was used to address the substantive research questions. The approach consisted of two phases: a review of secondary data and the collection of quantitative and qualitative primary data. The method employed was an explanatory sequential design, whereby distinct forms of data assist in building cumulative evidence. Specifically, we began by undertaking a review of secondary data to explore the cybersecurity context and followed this with the collection and analysis of primary data from WCSOs and CSOs, utilizing online survey methods from WCSOs, and conducting in-person and online interviews with WHRDs in the Southeast Asian region.

Phase 1: Sought to address Research Question 1 (what is the cybersecurity posture of WCSOs and WHRDs in Southeast Asia?) and comprised a review of the contextual influences on cybersecurity in Southeast Asia focused on civil society operations, human freedom, gender inclusivity and cybersecurity policy.

Phase 2: Sought to address Research Question 2 (how cyber-resilient are WCSOs and WHRDs in Southeast Asia?) and included the collection of survey data from those employed in WCSOs and CSOs in six target countries in the regions and a series of interviews with self-identified WHRDs.

Findings of each phase are discussed subsequently in sections dedicated to each Research Question. These are followed by an integration of insights to obtain a broader understanding of the needs of WCSOs and WHRDs in the region in protecting against cyber risks and promoting cyber resilience.

6.1 Participants and Procedures

6.1.1 SURVEY

A survey instrument was developed to assess the cybersecurity posture of CSOs in six Southeast Asian countries (Cambodia, Myanmar, Lao PDR., Philippines, Thailand and Viet Nam) using the analytical framework outlined in Table 2. The survey was translated into the local languages of the countries, and participants were given the opportunity to respond in their preferred language.

In addition to collecting demographic information concerning the participant and their organization, the survey included a series of validated and constructed measures to operationalize individual- and organizational-level experiences and perceptions of 1) cybersecurity assets, 2) cyber threats, 3) cyber vulnerabilities and 4) cyber resilience. The survey was hosted on the Qualtrics platform, with anonymous links generated and metadata intentionally not collected. This ensured that participants could not be identified and that their information would remain confidential.

A purposive sampling frame was utilized to identify participants for the online survey. This involved finding potential organizations through the following process:

1. **A systematic Google search**: A series of generalized Google searches were conducted to identify relevant women's organizations and networks in the region that could be potentially recruited to participate in the study.
2. **Document review**: Policy-related documents were reviewed in order to identify potential target organizations and individuals.
3. **Snowball sampling**: After the initial searches and outreach, additional potential organizations were identified through snowball sampling or through contact with organizations already identified.

In this process, identified WCSOs and CSOs were contacted via email to provide information about the study and to invite them to participate. Recruitment letters with an anonymous link to the survey were sent directly to participants and followed up with a reminder email. The survey was open for data collection between February and May 2023. In total, over 150 participants clicked on the survey link; 98 completed at least one of the questions. In the process of data checking, it was ascertained that 80 surveys (see Table 6) would be included in subsequent analysis on the basis of the completion of the majority of relevant measures.

6.1.2 SURVEY DEMOGRAPHICS

The average age of the participants was 39.71 (SD = 10.81). 42 sample participants identified as women (53 per cent), with 27 (34 per cent) identifying as men,

9 (11 per cent) as non-binary or as other gender, and 2 preferring not to disclose gender. The sample was highly educated, with 90 per cent having completed a postgraduate or undergraduate degree.

Regarding employment, the majority of respondents worked at the executive or senior levels (67 per cent). Employer organizations ranged in size from two people to 350 people (M = 40). The majority of organizations were led by women (63 per cent), and women comprised, on average, 67 per cent of staff employed in these organizations.

In order to identify whether the organization could be categorized as a WCSO, two key criteria were used:

Whether the organization had a specific mandate or vision to address or advocate for issues related specifically to women or girls (or gender more broadly); and/or

Whether women and girls were key clients of the organization.

To categorize organizations, participants were asked about the groups that they generally worked with, their main target group, the main topics they worked on and the mission 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.

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:

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

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

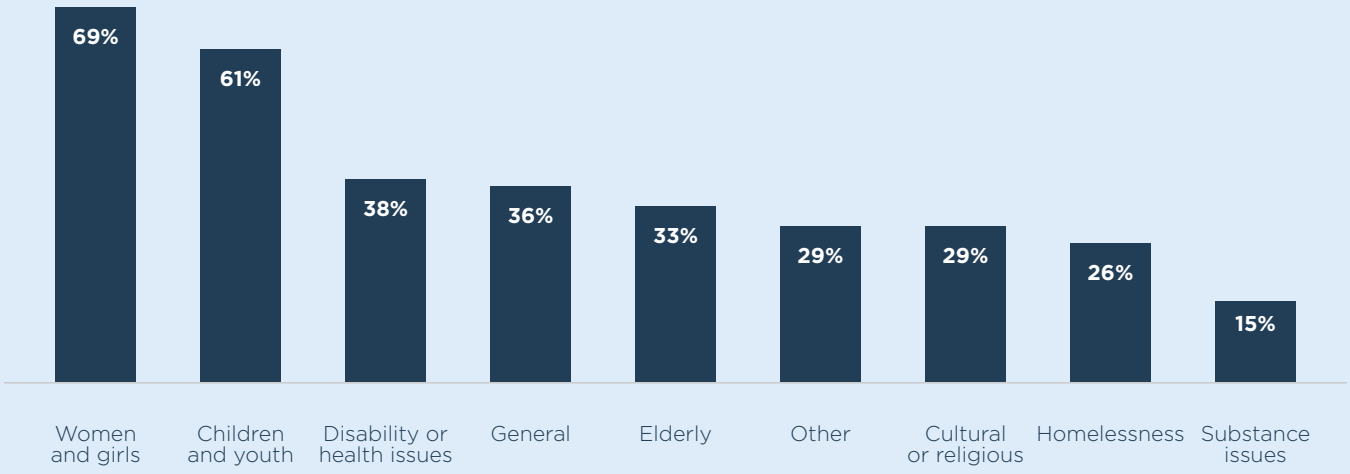
6.1.3 INTERVIEW PROCEDURE

A semi-structured interview schedule was developed to assess the cybersecurity experiences of WHRDs in the six Southeast Asian countries selected for the survey sample. Similar to the survey instrument, as well as collecting demographic information concerning the participant and their organization, the interview promoted a detailed investigation of the individual's cybersecurity assets, their experiences with cyber threats, their personal cyber vulnerabilities and the ways in which they were cyber resilient. They were also asked for their recommendations for others to increase their resilience.

To identify potential interview participants, individuals were invited from the WCSOs that were identified during survey recruitment, from networks of known WHRDs and from direct contacts made with individuals as a result of their high-profile activism in the region.

Identified WHRDs were contacted via email to provide study information and to invite them to participate. Recruitment letters were sent directly to participants,

FIGURE 12. CSO CLIENTELE[1]



1 Answers to the "other" category included a range of distinct groups, some of which could be categorized in those already defined such as; Indigenous, migrants, ethnic minorities (i.e, cultural or religious), but there were groups that were not adequately captured by the existing categories ,such as LGBTQI+, entrepreneurs, farmers and rural peoples, those in poverty and disaster survivors.

and a time was scheduled for the interviews. Each interview was audio recorded with the permission of the interviewee, and transcripts were processed initially through automated software and then checked by the researchers for accuracy. As per the survey, data collection took place between February and May 2023.

6.1.4 INTERVIEW DEMOGRAPHICS

Nineteen interviews were conducted with a total of 21 unique participants. Two interviews included two participating individuals. Five of the interviews were conducted in Thai and the rest in English. All interviews were audio recorded and transcribed for analysis into English. Three of the interviews were in-person, and the rest were conducted online through videoconferencing software. The interviews ranged in duration from 25 minutes to 1 hour and 45 minutes, with an average duration of approximately 40 minutes.

The sample comprised 20 women and one man from a diverse range of international, national and regional organizations. Most (18) of the participating WHRDs were not technically oriented in their roles, but the majority were in leadership roles, with eight being either directors, founders or presidents of their organizations, and eight being in management or adviser roles. Four of the participants were activists or campaigners, and one was an academic.

6.1.5 METHODOLOGICAL LIMITATIONS

Some limitations of the methodological approach are noted to highlight some constraints on generalizability. Civil society organizations were contacted for participation in the online survey via email using available information to the research team including through websites, civil society networks, and known contacts of the research team. Given the nature and sensitivities of the study, some participants may have been cautious about completing the information from an unknown source. The difficulty in collecting data for the online survey is reflected in the relatively small number of participants and unequal weighting in some countries as compared to others in the region. Notably, there are differences in the national context of individuals across the countries studied that could not be drawn out due to the sample size achieved. This also resulted in an unequal number of participants categorized as belonging to WCSOs as compared to CSOs. Due to lack of statistical power, assessments for statistically significant differences across these groups were not carried out. Unequal participation across countries was also notable in the interview with WHRDs. Critically, one of the major limitations in achieving representation in the interviews was language constraints. Specifically, interviews were able to be carried out in English or Thai (whereas the online survey provided all languages). This may have made participation more difficult for participants who were less familiar or comfortable discussing these topics in a non-native language. It is recommended that future research extend on the findings by collecting larger samples of participants working in civil society and as human rights defenders across the region to enable country specific analyses. Further, it is suggested that the sample should be broad enough to capture the experiences of those who advocate for women and girls, and well as those who engage with other types marginalised or vulnerable populations to assess differences and similarities in experiences.

TABLE 6. SAMPLE CHARACTERISTICS

COUNTRY	SURVEY SAMPLE	INTERVIEW SAMPLE
Cambodia	19	3
Lao PDR	6	-
Myanmar	8	-
Philippines	28	7
Thailand	12	10
Viet Nam	7	-
Regional	-	1
Total	80	21

APPENDIX 2.

REVIEW OF NATIONAL INDICATORS

The following section reviews a series of national-level indicators for the 11 Southeast Asian countries that make up the broader region. This analysis focuses on the four key areas:

- Digital progress and inclusion;
- Internet freedom;
- Gender equality in ICT; and
- Cybersecurity.

7.1 Digital Progress and Inclusion

Table 7 details the indicators that were reviewed for digital progress and inclusion. Within the broader Asia Pacific region, 64.3 per cent of the population used the Internet in 2022 (60.9 per cent of women and 67.5 per cent of men). This is similar to, but slightly lower than, the global average of 66.3 per cent (63.4 per cent of women and 69.2 per cent of men).[60] However, in reviewing the Southeast Asian region, we see a varied picture across-countries. Using the International Telecommunication Union Digital Data Development Dashboard[61] to assess the most recent gender-disaggregated Internet usage and mobile phone ownership data, it was found that in some countries, digital technologies are prevalent among both women and men (e.g. Brunei Darussalam, Singapore and Malaysia). However, other countries had very low levels of access and mobile phone ownership compared to the international average (e.g. Cambodia and Timor-Leste), and some had particularly high discrepancies across genders (e.g. Indonesia and Myanmar).[62]

Examining these data alongside developments in information and communication technology using the ICT Development Index (IDI) 2017[63] and the affordability of ICTs,[64] it is suggested that Internet access and mobile phone ownership are related to these indicators of ICT progress. Specifically, those with high Internet and mobile phone penetration were also highly ranked in the IDI globally, and Internet access was more affordable, with Singapore and Brunei Darussalam showing high levels of digital progress. In contrast, those countries with low Internet access and mobile phone ownership also tended to be ranked lower on the IDI and be less affordable to access the Internet (particularly Cambodia and Lao PDR).

7.1.1 INTERNET FREEDOM

Two indicators from Freedom House Global[65] on media and expression and Internet freedom were reviewed (see Table 8 for full information). The scores on media and Internet freedom show relatively low levels of freedom as measured by these indicators in general, but some countries were lacking data on one or both of these measures, so it is difficult to make clear comparisons. Notably, none of the countries were rated as being "free" based on the Internet Freedom score, although Indonesia, Malaysia and the Philippines all had relatively high levels of freedom and were considered "partially free." Three of the countries (Myanmar, Thailand, and Viet Nam) rated as "not free" also had relatively low levels of media freedom of expression.

60 https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
61 https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx
62 Lao PDR, Philippines, and Timor-Leste did not have gender disaggregated data on Internet use and mobile phone ownership.
63 The IDI is a composite measure of ICT access, use, and skills https://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017byregion-tab
64 Measured by the ITU Price Baskets Data-only mobile-broadband basket (2gb) 2022 which refers to the cheapest plan providing at least 2gb of high speed data over a 30 day period of time.
https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/IPB.aspx
65 The Freedom House Global Freedom score and Internet Freedom statuses and scores are reported https://freedomhouse.org/explore-the-map?type=fiw&year=2023

TABLE 7. DIGITAL PROGRESS AND INCLUSION INDICATORS IN SOUTHEAST ASIA

COUNTRY	WOMEN % USING THE INTERNET	MEN % OF USING THE INTERNET	% WOMEN'S MOBILE PHONE OWNERSHIP	% OF MEN'S MOBILE PHONE OWNERSHIP	IDI 2017 VALUE (GLOBAL RANK)	% OF GNI FOR BROADBAND PER CAPITA
Brunei Darussalam	100%	92%	99%	91%	6.75 (53)	0.28
Cambodia	52%	53%	71%	72%	3.28 (128)	2.42
Indonesia	59%	65%	61%	71%	4.33 (111)	0.85
Lao PDR	62%		-	-	2.91 (139)	2.67
Malaysia	96%	97%	97%	98%	6.38 (63)	0.98
Myanmar	19%	29%	57%	68%	3.00 (135)	1.67
Philippines	53%		79%		4.67 (101)	2.04
Singapore	97%	97%	88%	90%	8.05 (18)	0.22
Thailand	84%	86%	86%	87%	5.67 (78)	1.40
Timor-Leste	39%		-	-	3.57 (122)	4.59
Viet Nam	72%	77%	77%	78%	4.43 (108)	0.49

TABLE 8. INTERNET FREEDOM INDICATORS IN SOUTHEAST ASIA

COUNTRY	FREEDOM OF MEDIA AND EXPRESSION[66]	INTERNET FREEDOM SCORE[67]	INTERNET FREEDOM STATUS[68]
Brunei Darussalam	2.5	-	-
Cambodia	2.5	43	Partly Free
Indonesia	7.5	49	Partly Free
Lao PDR	-	-	-
Malaysia	5.0	59	Partly Free
Myanmar	2.5	12	Not Free
Philippines	2.5	65	Partly Free
Singapore	5.0	54	Partly Free
Thailand	2.5	39	Not Free
Timor-Leste	7.5	-	-
Viet Nam	-	22	Not Free

7.1.2 GENDER EQUALITY

To assess this indicator, a series of measures from the Global Gender Gaps Index[69] were reviewed alongside shares of women completing tertiary-level ICT education (see Table 9).[70] Taken together, these indicators shed light on the status of women's social and economic participation across the Southeast Asian region.

The overall ratings on gender equality highlight gender disparities across many countries in the Southeast Asian region, with the Philippines, Singapore, Lao PDR, and Timor-Leste rated relatively high and Brunei Darussalam, Malaysia and Myanmar rated relatively low on gender equality. Countries with higher overall gender equality tended to also be ranked higher in economic participation and educational attainment. Notably, however, overall ratings on health and security, as well as political empowerment, were more varied. Regarding gender

66 Calculation of this metric is published by the Human Development Index (see https://www.cato.org/human-freedom-index/2022) and is an aggregate of issues concerning censorship and political pressures in media. It ranges from 0 being the lowest levels of freedom and 10 being the highest.
67 Calculation of the score is based on an accessing of obstacles to access, limits on content, and violations of user rights. The total scores ranges from 0 being the lowest levels of freedom and 100 being the highest. See https://freedomhouse.org/reports/freedom-net/freedom-net-research-methodology for more information.
68 Where total scores on Internet Freedom range 0-39 this is classes as "not free," 40 – 69 as "partially free" and 70 – 100 as "free."
69 https://www.weforum.org/reports/global-gender-gap-report-2022/
70 https://genderdata.worldbank.org/indicators/uis-fgp-5-t8-f600/

equality among ICT graduates, it was found that Myanmar was the only country with over half of all graduates being women; five countries were between 40 per cent and 50 per cent (Brunei Darussalam, Lao PDR, Malaysia, Philippines, Thailand). The percentage of women graduates in ICT Tertiary was less than 40 per cent in four countries: Cambodia, Indonesia, Singapore and Viet Nam.

TABLE 9. GENDER EQUALITY INDICATORS IN SOUTHEAST ASIA

COUNTRY	GENDER EQUALITY OVERALL (RANK)	ECONOMIC PARTICIPATION (RANK)	EDUCATIONAL ATTAINMENT (RANK)	HEALTH AND SURVIVAL (RANK)	POLITICAL EMPOWERMENT (RANK)	FEMALE % OF GRADUATES IN ICT TERTIARY (YEAR)
Brunei Darussalam	.680 (104)	.726 (49)	.997 (48)	.966 (104)	.031 (144)	41.9% (2018)
Cambodia	.690 (98)	.710 (61)	.966 (105)	.978 (42)	.107 (121)	8.4% (2015)
Indonesia	.697(92)	.674 (80)	.972 (102)	.970 (77)	.169 (90)	34.7% (2018)
Lao PDR	.733 (53)	.883 (1)	.958 (109)	.975 (55)	.116 (116)	40.8% (2018)
Malaysia	.681 (103)	.656 (88)	.995 (56)	.972 (68)	.102 (123)	46.0% (2018)
Myanmar	.677 (106)	.637 (101)	.977 (96)	.980 (1)	.114 (118)	67.3% (2018)
Philippines	.783 (19)	.794 (16)	.997 (46)	.979 (30)	.360 (35)	48.1% (2017)
Singapore	.734 (49)	.765 (28)	.993 (65)	.963 (123)	.217 (66)	32.2% (2017)
Thailand	.709 (79)	.795 (15)	.979 (92)	.978 (37)	.084 (130)	47.9% (2016)
Timor-Leste	.730 (56)	.721 (55)	.977 (95)	.973 (66)	.250 (55)	-
Viet Nam	.705 (83)	.751 (31)	.985 (88)	.950 (141)	.135 (106)	26.4% (2016)

7.1.3 CYBERSECURITY

Cybersecurity has been defined differently according to each country's national context. Several indicators were reviewed in order to measure performance and reflect the current cybersecurity environment for the Southeast Asian region. These indicators included the National Exposure Index (NEI)[71] and a series of indicators from the Global Cybersecurity Index (GCI).[72] See Table 10 for further information.

Countries with high ratings on the NEI, which measures the risks posed by deliberate, wide-scale attacks to core Internet services, tended to also have high scores on the overall GCI, which is a more comprehensive measure designed to outline national cybersecurity readiness in a multidimensional way. Specifically, Singapore was ranked the highest and Timor-Leste the lowest on both measures, with the other countries' relative ranking ranging from very low to moderate levels. Reviewing the specific indicators on the GCI did show some interesting patterns. Despite Timor-Leste lacking data, most countries in the Southeast Asia region had high levels of legal and regulatory measures in place to respond to cybersecurity challenges, with 6 of the 11 countries rating above 18 on a scale with a maximum of 20. On this indicator, Cambodia, Lao PDR and Myanmar scored relatively low. Similar results were apparent for the other indicators as well, although there was more variation across the countries. Notably, the Philippines was found to have strong legal frameworks for cybersecurity, and Thailand was found to have relatively strong organizational measures, but both were weaker on other indicators.

Despite a range of differences across the region in terms of the national indicators reviewed here, there are some key patterns to be noted. Specifically, Singapore was rated high on most of the indicators compared to other countries in the region, particularly in digital progress and inclusion and cybersecurity, but less so on freedom. Whereas Cambodia, Lao PDR and Myanmar had relatively lower ratings on all of the indicators. A similar result is noted for Timor-Leste, although there was a substantial amount of missing data for that country. Results also indicate that gender disparities persist in the region both in terms of gender equality indicators and digital access.

71 https://exatel.pl/en/knowledge/blog/articles/national-exposure-index-report-onlie-threats/
72 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

TABLE 10. CYBERSECURITY INDICATORS IN SOUTHEAST ASIA

COUNTRY	NATIONAL EXPOSURE INDEX RANK	GLOBAL CYBERSECURITY INDEX (GCI) SCORE (RANK)	LEGAL MEASURES (GCI)	TECHNICAL MEASURES (GCI /20)	ORGANIZATIONAL MEASURES	CAPACITY DEVELOPMENT MEASURES (GCI)
Brunei Darussalam	48	56.07 (85)	14.06	14.19	10.84	12.85
Cambodia	95	19.12 (132)	7.38	2.50	1.69	3.29
Indonesia	26	94.88 (24)	18.48	19.08	17.84	19.48
Lao PDR	116	20.34 (131)	11.77	3.27	-	1.23
Malaysia	41	98.06 (5)	20.00	19.08	18.98	20.00
Myanmar	141	36.41 (99)	9.39	3.64	4.71	8.92
Philippines	57	77.00 (61)	20.00	13.00	11.85	12.74
Singapore	25	98.52 (4)	20.00	19.54	18.98	20.00
Thailand	24	86.50 (44)	19.11	15.57	17.64	16.84
Timor-Leste	186	4.26 (173)	-	-	-	-
Viet Nam	28	94.55 (25)	20.00	16.31	18.98	19.26

NOTE

Research supported by

Ministry of Gender Equality and Family

Australian Government

CYBER & CRITICAL TECH COOPERATION PROGRAM

UNU Macau

The United Nations University Institute in Macau (UNU Macau) is a United Nations global think tank conducting research and training on digital technologies for sustainable development, encouraging data-driven and evidence-based actions and policies to achieve the Sustainable Development Goals.

UN University Macau
Casa Silva Mendes, Estrada do Engenheiro Trigo No.4
Macau SAR, China

www.unu.edu/macau
www.twitter.com/UNUMACAU
www.facebook.com/unumacau
weibo.com/u/2698789630

UN WOMEN

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