DIGITAL SECURITY
FOR HIGH-RISK USERS IN THE ASIA-PACIFIC

NEEDS ASSESSMENT REPORT

ASIACENTRE

Digital Security for High-Risk Users in the Asia-Pacific

Needs Assessment Report

Asia Centre

2024

Asia Centre
65/168, Chamnan Phenjati Business Center Building,
20th Floor, Rama 9 Road,
Huai Kwang, Huai Kwang,
Bangkok, 10310, Thailand
contact@asiacentre.org

CONTENTS

Abbreviations V

Executive Summary VI

1. Introduction 1

1a. Methodology 1

1b. Key Terms 1

1c. Rise in Online Advocacy for Public Accountability 2

2. Digital Security Issues in the Asia-Pacific 4

2a. Legal Frameworks Regulating the Digital Sphere 6

2b. Online State Surveillance 8

2c. Information Operations 9

Doxxing 9

Cyber Troops 10

Gender-based Online Harassment 11

3. Protections Against Digital Security Threats 12

3a. Approaches to Digital Security Monitoring and Evaluation 12

3b. Existing Digital Security Measures 14

3c. Strengthening Digital Security Practices 16

Making Digital Security a Priority 16

Institutional Capacity-building 17

Capacity-building Opportunities for Individuals 17

4. Recommendations 21

5. Conclusion 23

Bibliography 25

Annex 32

ABBREVIATIONS

AI	Artificial Intelligence
APPI	Act on the Protection of Personal Information (2003) (Japan)
ASEAN	Association of Southeast Asian Nations
COVID-19	Coronavirus disease 2019
CSO	Civil Society Organisation
DDoS	Distributed Denial-of-Service
(I)NGO	(International) Non-governmental Organisation
IO	Information Operation
IOT	Internet-of-Things
KII	Key Informant Interview
LGBTQI+	Lesbian, Gay, Bisexual, Transgender, Queer, Intersex (and other)
M&E	Monitoring and Evaluation
MFA	Multi-Factor Authentication
OST	Open and Secure Technology
PECA	Prevention of Electronic Crimes Act (2016) (Pakistan)
PGP	Pretty Good Privacy
POFMA	Protection from Online Falsehoods and Manipulation Act (2019) (Singapore)
PRC	People's Republic of China
US	United States
VPN	Virtual Private Network

EXECUTIVE SUMMARY

Since the mid to late 2000s, the internet has profoundly impacted the social, economic, and political spheres of the Asia-Pacific region. As of 2024, about 66% of the population in South, East, and Southeast Asia are internet users, representing nearly 52.7% of the global user base (Kemp, 2024), while social media penetration stands at 60% in the Asia-Pacific region and continues to grow steadily (DMFA, 2024).

However, the increased use of the internet and social media has been accompanied by a rise in risks for users, especially those engaged in advocacy for public accountability. In 2022, the Asia-Pacific region accounted for 31% of global cyberattacks, with governments and their proxies being among the main perpetrators. These digital security threats impact a wide range of actors. Governments with strong democratic and liberal values, such as Taiwan, are frequent targets, with opposition parliamentarians and politicians in other jurisdictions facing intercepted communications and compromised data. Civil society organisations and rights defenders are also victims of these attacks due to their calls for government public accountability.

These online attacks underscore the need to bolster digital security training to safeguard all internet and social media users effectively, especially those in the high-risk user category. While digital security training is available, these efforts must be continuously updated and strengthened to ensure digital safety keeps up with changes in technology and digital threats.

Towards this end, this needs assessment was undertaken to map the contemporary sources of digital threats, the current mitigation strategies, and what more could be done to improve the situation. Using data from desk research, an online survey and key informant interviews, this needs assessment report addresses the need for enhanced digital security training in the Asia-Pacific by identifying three clusters of digital security threats faced by high-risk users in the region:

First, governments have enacted laws to regulate information creation, sharing and access, targeting hate speech, disinformation, defamation, and harmful content. While the issues that these legal tools seek to address are real concerns, many individuals from high-risk groups often face repercussions under these regulations, especially when governments use these tools against those who call for government public accountability.

Second, governments and their proxies have increased their efforts to monitor the online behaviour and activities of high-risk users to collect sensitive information. This systematic digital surveillance, conducted by national and foreign government agencies, encompasses deploying hacking and spyware tools to monitor online traffic, social media engagement, email correspondence, and other digital interactions. The intelligence gathered through these measures are used against those who advocate for public accountability.

Third, information operations that involve activities aimed at shaping and manipulating the information environment, particularly during politically active events such as protests, national elections, and the enactment of controversial legislation. These operations often utilise cyber troops and internet trolls to conduct disinformation campaigns online, aiming to undermine the credibility of their targets. They also include attacks aimed at websites and applications, disabling critical information in the lead-up to or during elections.

After identifying the above key sources of online threats, the report outlines the strategies that these high-risk users have adopted to date to counter these digital security challenges while highlighting their shortcomings. In terms of assessing online threats, the research shows while there are efforts to monitor and evaluate (M&E) threats, which are both reactive and proactive, overall, the approach is ad hoc and lacks a formal structure and process. In terms of mitigation efforts, what is commonly used are digital software solutions such as VPNs and multi-factor authentication to secure technologies and training programmes, but more needs to be done as gaps persist.

For instance, although there is a certain degree of awareness about digital security, it is a topic that is not mainstreamed or prioritised, both at the individual and institutional levels. In this context, inconsistencies on the monitoring of digital devices and limited digital hygiene among high-risk users remains as a crucial problem. This puts individuals, as well as the organisations and institutions they represent, at risk – in the digital sphere and, at times, physically.

The report concludes with a set of recommendations to strengthen digital security training opportunities. They focus on providing contextualised training that recognises how socio-political environments influence security landscapes. This approach includes integrating region-specific case studies to resonate with trainees' experiences, bolstering monitoring and evaluation systems to proactively identify vulnerabilities and equipping users with practical skills to mitigate threats such as phishing and DDoS attacks. It also emphasises the adoption of open-source technologies to build robust digital defences that can adapt to evolving risks effectively.

Adopting these recommendations is key for organisations and individuals developing digital security training programmes which should be reviewed and updated periodically. This will go a long way in ensuring the online safety and security of high-risk users, particularly those advocating for public accountability.

1. Introduction

Since the early 2000s, the Asia-Pacific region has seen a significant rise in internet users, leading to positive developments such as greater information diversity, enhanced political mobilisation, and improved tools for public accountability. Yet, it has also led to a sharp increase in digital security threats against high-risk users seeking public accountability and political change. Examples include phishing attacks, the interception of communications, the use of ransomware, and doxxing, among others. This report examines these threats, which stem from legal frameworks, state surveillance, and information operations. It also highlights the limited resources and inadequate digital hygiene practices that hinder protection efforts and offers recommendations to improve digital security through enhanced training.

1a. Methodology

The drafting of this report followed a three-stage process. The first stage, conducted from April to June 2024, involved desk research to explore the digital security landscape and sharpen the research focus. This phase aimed to identify gaps in existing knowledge, which the report seeks to address. Secondary sources, such as reports from international non-governmental organisations (INGOs), local civil society organisations (CSOs), technology companies, and news outlets, were reviewed.

In the second stage, from June to August 2024, the Research Team gathered primary data to fill the identified gaps. This included administering an online survey across the 12 countries covered in the report, with 67 respondents fully completing the survey. The Team used data from this survey to obtain an overview of the main types of digital security threats faced by high-risk users and what type of security measures they had in place. Then, 13 key informant interviews (KIIs) were conducted with participants from all target countries to obtain their lived stories about digital security and strengthen the nuances from the literature review and the survey.

Finally, the report underwent internal review by the Asia Centre Team and was presented to Google Asia-Pacific for feedback. Revisions were made accordingly, completing the review process.

1b. Key Terms

The following key terms are essential for understanding digital security in the Asia-Pacific:

High-risk Users: Individuals or organisations who maintain a significant online presence and use digital tools to actively advocate for public accountability concerning social and political policies. Due to their public facing online advocacy, they are often subject to online threats and attacks. This group includes parliamentarians, government officials, representatives from electoral and human rights commissions, members of political parties, lawyers, activists, human rights defenders, sexual minorities, and journalists.

Digital Threats: Any malicious activity to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorised access to a network, computer system or digital device.

Digital Security: A set of practices and tools used to safeguard personal data and online identity from unauthorised access, usage, disclosure, disruption, modification, or destruction.

Digital Hygiene: Digital hygiene involves adopting practices and habits to safeguard personal information and devices from cyber threats, including using strong passwords, enabling two-factor authentication, updating software, and being cautious of phishing attempts.

1c. Rise in Online Advocacy for Public Accountability

Since the mid to late 2000s, the internet has become ubiquitous, having a deep impact on social, economic, and political realms worldwide (Kemp, 2024). By 2023, approximately 5.35 billion people out of 8.08 billion globally were connected to the internet, marking a significant milestone two decades after its widespread adoption began (Ibid.). The surge in internet usage has been particularly prominent in the Asia-Pacific (refer to Table 1), leading to the widespread adoption of social networking sites, largely facilitated by the widespread availability of smartphones (refer to Table 2).

Table 1: Internet Users in South, Southeast and East Asia

Region	Share of Global Internet Users	Region-wide Internet Penetration
South Asia	18.5%	47.4%
Southeast Asia	10%	75.6%
East Asia	24%	74.3%

(Kemp, 2024)

Table 2: Social Media and Mobile Connectivity in Relation to the Total Population

Region	Social Media Users	Mobile Connectivity
South Asia	32.4%	85%
Southeast Asia	60.3%	129%
East Asia	74%	125%

(Kemp, 2024)

This digital transformation has brought numerous opportunities for various actors. One of the overarching benefits of the digital sphere's development has been in the realm of online advocacy by public officials, parliamentarians and political parties, and civil society activists.

This has been evident in various contexts. For example, the Human Rights Commission of Pakistan (HRCP) (nd.) uses digital media to advance human rights and accountability through various campaigns, including seminars, workshops, and online advocacy, addressing issues such as women's rights, children's rights, and the rights of vulnerable groups. HRCP issues real-time statements and detailed reports on topics like press freedom via their website and social media, reaching a broad audience. They also engage government officials through online forums and webinars and use social media to directly pressure policymakers on issues such as police brutality. These digital strategies help HRCP document abuses, advocate for change, and mobilise global support.

Digital activism in the Philippines has played a crucial role in exposing human rights abuses and advocating for reform. Organisations such as the Center for International Law and Policy (nd.) have effectively leveraged digital platforms to document and raise awareness about issues including extrajudicial killings, police brutality, and the suppression of dissent under the Duterte administration (CenterLaw, 2023). These digital efforts have enabled them to reach a broader audience, mobilise public support and put pressure on national and international bodies to address these concerns. Through detailed reports, social media campaigns, and online advocacy, these organisations have been instrumental in highlighting the scale and impact of human rights violations in the country.

The internet, particularly the growth of social media, has also improved the capacity of parliamentarians and political parties to disseminate information, communicate with the public, and mobilise electorates (Raaban & Muhammad, 2023). In 2014, India's Bharatiya Janata Party, recognising this potential (The Times of India, 2022), utilised WhatsApp groups, the party targeted specific audiences using demographic and socio-economic data analytics (Singh, 2019), allowing the party to circulate a personalised "Letter from the Prime Minister" via WhatsApp, highlighting his achievements and seeking feedback and support from voters (The Economic Times, 2024).

In the run-up to Taiwan's 2024 presidential election, Threads surged in popularity due to its light-handed political content moderation, setting it apart from other social media platforms (Yang, 2024a). Democratic Progressive Party supporters found it more conducive to reaching broader audiences compared to platforms like Facebook and Instagram, which face issues with bots, disinformation, and contentious moderation policies (Yang, 2024b). By blending political discourse with lifestyle content, party supporters effectively utilised Threads as a mobilisation tool, leading to it becoming the most downloaded app in both the Apple and Android stores in Taiwan within three months.

In Thailand's 2023 general election, Move Forward Party secured victory with 151 seats, propelled by its adept social media strategy, notably on TikTok. Organic supporters played a pivotal role in amplifying the party's message through user-generated content (The Business Times, 2023). The Party shared approximately 200 TikTok videos during the campaign each garnering millions of views, with some reaching 10 million. Within three months, they amassed over 300 million views, showcasing content from party members, staff and supporters, culminating in nearly 4 billion views (Adair, 2023).

The internet has also improved advocacy. In 2021, a group of Indian students in Southern Goa's Chandor village used Facebook, Instagram, and Twitter to mobilise thousands of people to protest against infrastructure projects that would turn their locality into a regional coal hub, affecting the nearby national park and wildlife sanctuary (Naik, 2021). The planned projects were spearheaded by Gautam Adani – an Indian billionaire with close ties with Prime Minister Narendra Modi (Ellis-Petersen, 2023). An Instagram page Mollem Memory Project, dedicated to the movement's activism, grew from 4 followers to 4,500 people in a few months (Ibid.).

During the Coronavirus disease 2019 COVID-19 pandemic in 2020, online protests erupted against the appointment of Hiromu Kurokawa as prosecutor-general in Japan, viewed as compromising judicial independence due to his close ties with the government (Uchida, 2023). A tweet by a feminist protesting the appointment went viral, garnering over 4.7 million shares within days, leading to government reversal and Kurokawa's resignation over a violation of COVID-19 travel and health policies (Kyodo News, 2020).

In essence, the digital transformation in the Asia-Pacific has unlocked numerous opportunities for both state and non-state actors to enhance their online advocacy. However, there is a stark contrast between the potential benefits of the internet – such as improving governance, voter mobilisation, and public accountability – and the associated risks. While the internet and social media can be powerful tools for driving positive change, it also exposes users, particularly those engaged in governance and advocacy, to significant threats. These individuals, labelled "high-risk users", are especially vulnerable due to the nature of their online activities. The upcoming chapter will examine how their efforts are compromised by threats such as restrictive laws, digital surveillance, and information operations, highlighting how these factors undermine the safety and effectiveness of their online advocacy.

2. Digital Security Issues in the Asia-Pacific

In 2022, the Asia-Pacific region saw a significant increase in global cyberattacks, constituting 31% of total incidents worldwide. Nearly half of these attacks (49%) involved communications interceptions, compromising sensitive information (Positive Technologies, 2023) and primarily targeted government agencies, comprising 22% of all attacks (Infoxchange & Tech Soup Asia-Pacific, 2023). There are also instances of cyber-attacks targeting parliamentarians. In October 2023, Apple issued warnings to several prominent Indian opposition leaders and journalists, indicating that their iPhones were likely targeted by "state-sponsored attackers". This notification raised concerns about the safety and privacy of these individuals, particularly those seeking public accountability (Aljazeera, 2024). Yet, the government sector is not the only target of cyber-attacks. Between 2022 and 2023, one in six non-profit organisations in the Asia-Pacific reported facing digital security threats (Infoxchange & Tech Soup Asia-Pacific, 2023).

Amid these challenges, two Asia Centre's publications highlight the growing concern over digital security and urge all stakeholders to take necessary precautions against digital threats. On the one hand, *Digital Security and Human Rights Defenders in the Asia-Pacific* (2023) evaluates the adoption of digital security tools and measures by changemakers in the region to counter online threats, particularly in the face of increasing state surveillance. On the other hand, *Digital Security & Human Rights Defenders Landscape* (2023) examines the challenges faced by human rights defenders (HRDs) in the Asia-Pacific in the digital era, assessing the effectiveness of National Human Rights Institutions (NHRIs) in protecting HRDs.

This chapter contextualises digital security in the Asia-Pacific by examining three primary sources of threats faced by high-risk users: restrictive legal frameworks, online state surveillance, and information operations. Together, these sources of threats form the bulk of challenges high-risk users face, which will in turn inform the digital security needs discussed in Chapter 3.

Sources of Digital Security Threats

Perpetrators of Digital Security Threats

State Actors

State actors pose digital security threats through both legal measures, by passing restrictive laws, and using non-legal tactics such as surveillance and information manipulation. These actions restrict freedoms, invade privacy and intimidate high-risk users.

Non-state Actors

Non-state actors, such as troll armies and PR agencies, play a crucial role in online threats. They manipulate information, harass high-risk users, conduct cyberattacks, and spread harmful rhetoric. Often affiliated with public security agencies, political parties, or foreign interests, these actors amplify digital insecurity.

Foreign Entities

Foreign entities, often supported by foreign governments, conduct surveillance and orchestrate attacks on government websites, alongside propaganda campaigns. These activities specifically target politicians and activists who hold views contrary to foreign interests, especially during election periods.

Victims of Digital Security Threats

State Institutions

State institutions with inadequate security measures and members of political opposition, including parliamentarians and party members who challenge ruling elites, are often targets of online harassment and cyberattacks. This also includes members of election and human rights commissions.

HRDs & Activists

Human rights defenders and activists who call for public accountability over issues such as corruption, human trafficking, torture, enforced disappearances, and unauthorised government actions are similarly at risk. Whistleblowers exposing corruption and other wrongdoings also face significant digital threats aimed at silencing them, including legal measures and state surveillance.

Minority Groups

Minority groups and their advocates are particularly vulnerable to online harassment based on race or gender. They are often targeted through information operations aimed at intimidating and silencing them. These operations exploit their marginalised status and the pervasive discrimination they face, hindering their ability to speak up and advocate for their rights.

Journalists

Journalists and media personnel, particularly women journalists and those covering sensitive or controversial topics, frequently face digital threats as a result of their investigative and reporting activities.

2a. Legal Frameworks Regulating the Digital Sphere

In the Asia-Pacific region, governments have implemented various laws to regulate online information creation, sharing, and consumption. These regulations aim to address issues like hate speech, disinformation, and defamatory content. However, high-risk users, such as those relying on social media and messaging platforms for their work, often find themselves targeted and harassed under these laws.

This section examines how internet regulations are used to control content in the digital space, with examples from Pakistan, Singapore, and Japan. Understanding these specific laws, their implications for users, and how they are enforced is essential for high-risk users. This awareness not only aids in navigating online activities more effectively but also plays a crucial role in enhancing digital security for those most vulnerable to these regulations.

Pakistan's Prevention of Electronic Crimes Act (PECA) (2016) was implemented to address the increasing issue of cybercrime. Nevertheless, its broad and vaguely defined rules have created worry and doubt among high-risk users striving to hold government officials accountable for their actions. Apprehensions have been raised about its potential to restrict freedom of expression. PECA has been criticised due to its ambiguity since it grants authorities sweeping power to monitor, intercept and censor online content deemed unlawful. Yet, the definition of *unlawful* remains vague. This lack of clarity enables authorities to subjectively interpret the law, often targeting content critical of the government or its policies.

In 2017, Zafar Achakzai, a well-known Pakistani journalist, faced accusations of sharing anti-army content on social media. He was charged with cyber terrorism and defamation of the military, based on Facebook posts criticising the army's actions in the province of Balochistan. Achakzai's lawyer argued that his comments fell within his right to freedom of expression (Hashim, 2017).

PECA also empowers authorities to censor online content under Section 37, which grants extensive authority to the Pakistan Telecommunications Authority to censor or delete online content, limiting the freedom of speech outlined in Article 19 of the constitution. In 2018, social media platforms like Twitter and Facebook were temporarily blocked amidst anti-government protests (Shahid, 2018). This incident highlights how PECA can be used to restrict opposing viewpoints and regulate the dissemination of information, especially amidst periods of political turbulence.

In May 2024, Pakistan established a new cybercrime investigation unit under the PECA. The newly established National Cyber Crime Investigation Agency is led by a director general appointed by the government for a two-year term, requiring significant expertise in relevant fields. Meanwhile, Pakistan's information minister has revealed plans for a new authority aimed at tackling online harassment and safeguarding digital rights (Saeed, 2024).

The case of Singapore serves as an example of the legal measures adopted to counter fake news. The rapid expansion of the digital realm has facilitated the creation and spread of disinformation. Social media and online platforms enable information to circulate swiftly. In response, governments have enacted fake news laws to tackle the dissemination of misleading content. However, these laws have faced criticism for potentially allowing governments to curtail people's rights, particularly freedom of expression. Ambiguous definitions and selective enforcement permit authorities to target those holding governments to account, potentially chilling public discourse.

In 2019, Singapore introduced the Protection from Online Falsehoods and Manipulation Act (POFMA) (2019) to tackle the dissemination of online falsehoods and manipulation that might undermine public welfare. This law empowers relevant government officials to legally label as "false" certain statements

and thereby mandating corrections, content removal, and the disclosure of information sources. POFMA's stated objective is to counter misinformation and disinformation, preserving the honesty of public discussions and shielding individuals and organisations from baseless accusations.

However, POFMA also threatens high-risk users, such as opposition party members, restricting their ability to express views freely without fear of repercussions. Proponents emphasise its role in maintaining social harmony and combating misinformation. Kenneth Jeyaretnam, leader of the Reform Party, received his sixth POFMA correction direction for alleging that ministers K Shanmugam and Vivian Balakrishnan received below-market rent for bungalows on Ridout Road. The government refuted these claims, citing investigations that stated the properties were rented at fair market value (CNA, 2024). In a tracker compiled in 2024 by independent journalist Kirsten Han, the information shows that in its five-year lifespan, the Act (POFMA) had been deployed at least 151 times (Han, 2024) (POFMA Tracker, Kirsten Han) highlighting its significant role in regulating calls for public accountability online. Notably, civil society activists, individual commentators, and opposition politicians top the list of those "POFMAed".

Beyond its impact within Singapore, POFMA has served as a model for some South Asian countries, such as Sri Lanka, prompting them to study the law and formulate their own versions (Economy Next, 2021). In January 2024, Sri Lanka passed the Online Safety Bill, which includes many provisions resembling those of POFMA (Aljazeera, 2024; Rajapakse, 2023). Conversely, South Korea attempted to pass its own fake news law in 2021, but the government ultimately withdrew the proposal following backlash from civil society actors who perceived it as a threat to media freedom (Gallo & Lee, 2021).

In Japan, the use of non-internet laws like defamation and information laws show how these pre-internet legal provisions are equally being used to govern online challenges, including online harassment, digital piracy, and the spread of harmful content on digital platforms.

Japan's Act on the Protection of Personal Information (APPI) (2003) safeguards individuals' personal data across various entities. It aims to balance privacy protection with legitimate data use for business and social purposes. The law mandates consent for data collection, specifies usage purposes, requires security measures, and limits data retention. Oversight falls under the Personal Information Protection Commission, though weak enforcement and exemptions for government agencies have drawn criticism. Strengthening enforcement and addressing government exemptions are crucial for comprehensive personal data protection under the law.

However, the APPI lacks robust enforcement mechanisms. The regulatory body overseeing APPI, the PPC, primarily relies on issuing recommendations for improvement (Paulger, 2022). However, these recommendations do not carry legal weight, potentially allowing those to be disregarded. Secondly, the APPI exempts certain government activities from its purview. This exemption raises concerns about unequal protection, as government agencies may not be subject to the same regulations regarding data collection and use as other actors like private companies. Such measures, while intended for public health purposes, could be misused without proper oversight under APPI. Without proper safeguards, the government could potentially collect and use personal data for purposes beyond its stated aims, infringing on individual privacy.

These shortcomings indicate that the APPI might not effectively protect individuals' privacy rights in all scenarios. While the Act establishes a framework for data protection, requires consent for the collection and use of sensitive data in most cases, and mandates security measures for personal information, the lack of robust enforcement and exemptions for government agencies raises concerns about its ability to achieve its goals.

While legal frameworks do not inherently constitute a digital threat, they are critical for contextualising digital security issues and understanding their legal implications across different jurisdictions, especially when they are weaponised against those advocating for public accountability. These frameworks become a crucial component of comprehensive and robust digital security training, as they help high-risk users navigate legal environments and mitigate potential risks effectively. Understanding the legal landscape is essential for developing strategies that not only address immediate digital threats but also ensure long-term compliance and protection within varying legal contexts.

2b. Online State Surveillance

Digital security threats to high-risk users often involve monitoring their online activities to gather information. Systematic surveillance and tracking of internet traffic, social media activity, email communications and various other digital interactions, by national and foreign agencies have raised significant privacy concerns (Hynes, 2021).

An example of online state surveillance is the utilisation of Pegasus, a spyware capable of intercepting online communications without users' consent. It employs "zero-click" technology whereby malware is installed on a device without requiring any user action from the target, such as clicking on a link. This allows the attacker to have access to data stored in the targeted device and could read, edit, leak, or delete the information (Kaspersky, nd.).

Governments in numerous countries worldwide have employed this software to clandestinely gather information from opposition forces and activists (APNews, 2024; Iwaniuk, 2024). The use of Pegasus by several Asian governments highlights that the region is not immune to online state surveillance, a concern shared by political opposition parties and human rights defenders.

In Thailand, for instance, one respondent (KII1) explained that pro-democracy activists in the country have been the target of surveillance using Pegasus. From October 2020 to November 2021, a period coinciding with nationwide political protests against pandemic mismanagement, at least 30 pro-democracy academics, activists, and civil society members were subjected to state surveillance through Pegasus spyware (iLaw, 2024; Scott-Railton et al., 2022). Many of the targeted individuals were leaders of youth-led political movements advocating for structural reforms regarding the monarchy. These surveillance efforts were allegedly aimed at gathering information on protest locations, schedules, and sources of financial support. As a result of their political activism, some protest leaders faced charges of lèse-majesté offences.

The same respondents added, "I am not sure whether this is still ongoing, but it is something that I know that the civil society and pro-democracy movement is still cautious about" (KII1).

Another case of online state surveillance – particularly communications interception – in Southeast Asia occurred in Cambodia. In 2021, during a Zoom meeting among exiled opposition members of the now-defunct Cambodia National Rescue Party, then-Prime Minister Hun Sen unexpectedly intruded on the call. His presence conveyed a veiled threat, suggesting that the participants' activities were closely monitored by the government. Additionally, Hun Sen advised the exiled members against returning to Cambodia, implying potential repercussions if they did so. This incident underscored the intrusive nature of state surveillance in Cambodia and raised concerns about privacy and freedom of expression under the country's political leadership (Phon & Turton, 2021).

In South Asia, Indian journalists Siddharth Varadarajan and Anand Mangnale were targeted with Pegasus spyware on their phones in 2023. Varadarajan, the founding editor of The Wire, an online news media outlet, believed that he had been targeted due to his outlet's opposition to the detention

of the NewsClick editor in New Delhi under a politically motivated accusation of receiving funds from China (VOA News, 2023; Saaliq, 2023). Meanwhile, Mangnale, the editor at the Organised Crime and Corruption Reporting Project, commented that the attack came within hours after he sent investigative questions to Adani Group, whose founder is an ally to Prime Minister Narendra Modi, over alleged improper tax use and stock manipulation (VOA News, 2023; Reuters, 2024).

In South Korea, during the COVID-19 pandemic, the government implemented a robust contact tracing system to control the virus' spread, prompting worries about surveillance and privacy. This entailed logging GPS locations, social media activities, credit card transactions, and individuals' mobility history. Personal data would be disclosed to the public when a significant number of COVID-19-positive cases are identified in a single location. However, members of the LGBTQI+ community and queer activists, who often sought to maintain a low profile due to stigmatisation and homophobia, felt targeted by this health surveillance. They feared their identities might be forcibly revealed (Gitzen 2020; Gitzen & Chun, 2021). For example, a reported COVID-19 case from the Itaewon neighbourhood in Seoul, known for its nightlife, led to online hostility toward the LGBTQI+ community after the venues the person who tested positive visited were disclosed as gay clubs (Borowiec, 2020).

In addition to government surveillance of their citizens, there are instances where foreign entities or their supporters engage in surveillance. An expert from Taiwan (KII9) highlighted how members of the Taiwanese government, along with foreign activists and human rights defenders critical of China and supportive of Ukraine, face surveillance and potential targeting by groups aligned with Chinese and Russian interests. Furthermore, reports indicate that China has assisted countries such as Cambodia (Chandran, 2022) and Vietnam (KII10; Nguyen, 2022) in deploying extensive digital surveillance systems comprising CCTV cameras, drones, and Artificial Intelligence technologies to monitor activists and protesters. In Taiwan, concerns have been raised about the infiltration of Chinese-made surveillance tools, including CCTV cameras, under misleading circumstances, posing a significant threat to foreign digital surveillance (Huang, 2022).

The examples above show how surveillance has been misused and directed towards monitoring opposition forces. This has led to infringements on their right to privacy, interference with their advocacy efforts, and, in some cases, stigmatisation of citizens during public health emergencies.

2c. Information Operations

The third source of digital security threats is Information operations (IOs). It involves efforts to shape and influence the information landscape, particularly during politically significant events like national protests, elections and the passage of controversial laws. These operations often utilise agents such as cyber troops and internet trolls to orchestrate online disinformation campaigns aimed at undermining the credibility of their targets (Klingová, 2023). In South, Southeast, and East Asia, IOs represent a security threat to high-risk users, evidenced by the practice of doxxing, cyberattacks perpetrated by cyber troops, and gender-based online harassment.

Doxxing

According to several respondents (KII1, 2, 3, 4, 5, 6, 9, 11; 14), doxxing, a practice that is on the rise, is one of the most commonly-practised forms of discrediting high-risk users, which also increases their threats of being prosecuted. Doxxing refers to the act of "revealing identifiable [personal or sensitive] information about someone online" (Kaspersky, nd.), which often puts high-risk users in the spotlight of local authorities, facilitating their identification.

Doxxing has become a tool for malinformation linked to legal threats. Exposing civil society actors' identities (as well the identities of their close friends and family members (KII12)) has become a tactic by "cyber troopers" (KII1), often leading to legal consequences and sustained periods of interrogation by authorities (KII5, 6, 11). This can be seen with examples like the "Minion Army" in Thailand, a group that threatens to submit personal information of high-risk users to the police, facilitating the charging of these activists using laws such as lèse-majesté (Suphasan, 2021).

Another example is the trend of doxxing members of underrepresented groups – such as activists representing the Lesbian, Gay, Bisexual, Transgender, Queer, Intersex (among others) (LGBTQI+) community – who can be subjected to harassment and discrimination, and even prosecution in some countries, once they are identified by the public (KII4). In one case in Indonesia, the personal information organisers of an LGBTQI+ event were doxxed, leading to conservative religious groups issuing death threats and threats of legal prosecution (UCA News, 2023). The "outing" of LGBTQI+ groups, leading to arrests in countries where such sexual and gender orientations are prohibited, is also facilitated by doxxing (The Human Rights Campaign, 2017).

Doxxing also poses a significant risk for government agencies, as it involves the exposure of sensitive information that could potentially jeopardise national security or reveal confidential details (KII2, 3). In Taiwan, there has been a notable trend of hacking, leaking, and releasing sensitive official documentation by doxxing political figures and civil servants. This activity is suspected to be driven by geopolitical tensions, with actors potentially aligned with the People's Republic of China (PRC) being involved in these cyber operations (KII9; Chiu, 2023; Aljazeera, 2023).

Cyber Troops

Previously, in 2021, anti-corruption activists from the Indonesia Corruption Watch reported a surge in cyberattacks, ranging from their WhatsApp accounts being hacked to a Zoom conference being sabotaged with pornography (Lamb & Potkin, 2021). These cyberattacks were seemingly motivated by the earlier dismissal of 75 public officials from the Corruption Eradication Commission, who had failed a controversial civil service exam. This exam became mandatory after a transformation that changed the status of the Commission's employees from independent consultants to civil servants (Lane, 2021). The disruption to the conference occurred while members of the Indonesia Corruption Watch were engaged in a video conference discussing these dismissals (Lamb & Potkin, 2021).

Another illustration of the presence of cyber troops and the security risks they pose to high-risk users can be seen in Bangladesh. In 2021, the ruling Awami League reportedly trained tens of thousands of its party cadres to function as cyber troops, engaging in information operations in anticipation of the 2024 general election (Foyez, 2021). While the Awami League claimed this training was to counter disinformation from the opposition party, critics, however, pointed out that it had been used to control the official narratives on social media and harass or silence the views of opposition party members, especially when exposing policy lapses of the Awami League (Mahmud, 2021). Six months after the general election on 7 January 2024, an independent online media research platform, Dismislab (2024), claimed to have uncovered a network of 1,369 bots promoting the Awami League's policies on Facebook. These bots were responsible for over 21,000 coordinated comments in favour of the party, with the activity ramping up shortly before the 7 January national elections, which Dismislab alleges were won by the Awami League through rigging. During the July and August 2024 protests against Hasina's government, which caused her to flee, creating spam-free broadcast channels for urgent news and alerts was essential. These channels helped protesters gather and share information and instructions from student coordinators, improving organisation and coordination (Anjum, 2024).

It must also be noted that the aforementioned threats or sources of IOs can also be external. For instance, ahead of the 2024 presidential election in Taiwan, the PRC actively orchestrated a complex online disinformation campaign aimed at candidates of Taiwan's ruling Democratic Progressive Party (KII9). This disinformation included spreading rumours about the party's vice-presidential candidate Hsiao Bi-khim supposedly being a United States (US) citizen, as well as fabricating reports about joint efforts between Taiwan and the US to develop biological weapons targeting mainland China (Cheung, 2023; Köckritz, 2023). These false narratives often became intertwined with disinformation originating from within Taiwanese society itself. Suspicions arose around online journalist Lin Hsien-yuan, who was believed to have collaborated with Chinese interests, as he published a fraudulent popularity poll that placed pro-Beijing candidate Hou Yu-ih from the Chinese Nationalist Party in the lead (Lau, 2024).

Gender-based Online Harassment

In February 2024, Thai Member of Parliament Chonthicha Jangrew disclosed that she suffered from post-traumatic stress disorder due to prolonged exposure to online hate speech and sexually degrading messages stemming from her activist background demanding reform on the monarchy (Bunnag, 2024). Before assuming office in 2023, Chonthicha had been a youth activist advocating for structural reforms within the monarchy, a stance that led to her facing a total of 14 criminal charges, including the lèse-majesté offence (Trisuwan, 2020). Some of the harassment she has been subject to was reportedly carried out by the Internal Security Operation Command, a public security unit within the Thai armed forces, which allegedly employs fake social media accounts to disseminate disinformation and hate speech targeting high-risk groups (Asia Centre, 2023).

As the internet, social media and messaging applications become platforms for information sharing and public advocacy, this has resulted in increased harassment against high-risk groups due to their online behaviour. In 2020, Nepalese journalist Binu Subedi from Kantipur National Daily faced cyberbullying following her news report questioning the stability of the coalition government led by the Communist Party of Nepal and the well-being of workers during the COVID-19 lockdown (Nepal Press Freedom, 2020). Twitter (currently known as X) users affiliated with the party inundated Subedi's account with defamatory messages and misleading comments attacking her professional integrity (Ibid.). In 2022, a report by the Media Advocacy Group revealed that 88% of women journalists in Nepal, like Subedi, had encountered online violence at some point in their lives, with 53% indicating that such violence was linked to their profession (Media Advocacy Group, 2022).

In South Korea, anti-feminism takes the form of cyberbullying against alleged "feminists", driving some to the point of suicide (Kim & Lee, 2022; Nam, 2024). YouTube is the major platform for online hate speech and intimidation against women as pointed out by a key informant from the country (KII8). For example, a misogynistic video denouncing a woman activist due to her advocacy for gender equality gathered hundreds of thousands of viewers and thousands of comments including death threats (AFP, 2022). Others have been doxxed by male YouTubers who believed them to be man-haters. Anti-feminist YouTube accounts in South Korea, with thousands of followers, are actually profiting from the harassment as their hateful content generates more clicks and advertising revenue (Ibid.).

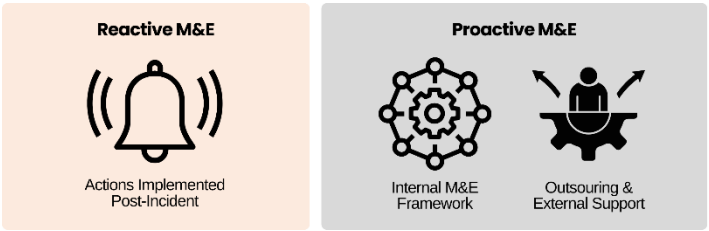
In essence, digital security in the Asia-Pacific region is compromised by several factors. Legal frameworks, initially designed to regulate the digital sphere, are frequently weaponised against high-risk users. State surveillance is intensifying, targeting specific actors to gather sensitive information, while information operations are escalating online harassment. Yet, the contextual nature of these threats requires further scrutiny. The next chapter will outline key high-risk users in target countries, examine the digital security threats they encounter, and propose strategies to enhance their protection.

3. Protections Against Digital Security Threats

This chapter delves specifically into the capacity and strategies adopted by high-risk users to manage these threats. It has three parts. First, it focuses on the approaches to monitor and evaluate digital security threats, identifying approaches that are reactive and proactive. Second, it outlines the various digital security strategies identified among respondents. Third, it analyses the shortcomings of such digital security measures. This forms the basis for the recommendations in Chapter 4 which can be nuanced for different users.

3a. Approaches to Digital Security Monitoring and Evaluation

Among all respondents involved in this research, all were aware of digital security issues, as elaborated in Chapter 2. This points to a high level of awareness among high-risk users in the region. However, what sets respondents apart is how they and the organisations they represent, as well as their partner organisations in the same field, address these threats. This section discusses the ways in which high-risk users monitor and evaluate (M&E) digital security risks, distinguishing between reactive and proactive approaches.



The first approach towards M&E is reactive. This approach involves individuals and organisations taking protective actions after an attack on digital security has occurred. These measures typically focus on quick-fix solutions aimed at assessing the damage and aiding in recovery. Examples of reactive cybersecurity protections include data recovery efforts, patching vulnerabilities, and updating security software (Sangfor Technologies, 2023). Therefore, this approach is characterised by a notable lack of efforts to evaluate current digital security threats, measures and associated practices in place; and, in some instances, an absence of them altogether.

As one informant observed (KII1), in their organisation, comprehensive M&E is usually undertaken only in response to specific alerts or notifications of security breaches. This method often prioritises corrective actions to resolve immediate issues rather than focusing on proactive strategies to enhance the overall digital security posture. Reinforcing this stance, another key informant from Nepal (KII6) characterised their organisation's current M&E methods as ad hoc, pointing out that they were still in the process of developing formal digital security guidelines. As this respondent said,

> To be honest, we have been discussing [...] about developing our digital security guidelines for our organisation. Currently, we are handling digital security on an ad hoc basis, thinking and implementing measures as needed without a formal structure (KII6).

Therefore, those who adopt this approach tend to react to digital security threats only after an incident has occurred or when a threat has been identified using existing security protocols. This reactive stance can leave them highly vulnerable and at higher risk when encountering new varieties of threats, compared to those who take a proactive approach – as explained below.

In contrast to the reactive approach, the proactive approach emphasises regularly identifying potential digital security vulnerabilities in advance of their exploitation. Examples of proactive measures include firewalls and threat detection systems, along with regular vulnerability assessments and employee training on proper cyber hygiene (Ibid.). Since the proactive approach is strategic and forward-looking, aiming to mitigate risks before they materialise, it is marked by systematic planning and consistent application of security practices designed to anticipate potential threats and counteract them before they can cause harm.

Based on the information provided by the participants, there are two distinct approaches towards adopting a proactive Monitoring and Evaluation (M&E) method: organisations or individuals with an existing – yet limited, in some instances – M&E framework and those who rely on external parties to provide the needed support.

The first sub-group comprises those with an established M&E plan. Within this group, organisations and individuals conduct periodic checks for vulnerabilities. High-risk users greatly benefit from taking a prompt and proactive approach to digital security threats. By regularising efforts to strengthen and maintain their digital security, they can develop a clear vision and maintain a safe environment tailored to their needs (KII5). This approach also allows them to swiftly identify and mitigate threats – often based on previous threats that have been experienced by high-risk users (KII12) – ultimately enhancing overall security measures.

Proactive cybersecurity can be cost-effective, saving valuable resources and time. Moreover, it enables high-risk users to better prepare for and mitigate risks (PRODRAFT, 2024); this benefit is multiplied in a working context where high-risk organisations regularly share instances of threats with each other to keep the network alert of possible security risks (KII12).

However, the interactions with respondents show that even among those who have a cybersecurity M&E plan, there is a certain degree of inconsistency due to a lack of clarity regarding the specific M&E criteria and the absence of an established routine or dedicated team for conducting regular assessments. Consequently, the effectiveness of existing plans to evaluate digital security threats is diminished.

This inconsistency is further exacerbated by the relative absence of a formal M&E process for all staff. For example, a respondent from Japan (KII7) explained that while their organisation has technical staff responsible for computer and software maintenance, they are unable to conduct an M&E of all of their staff's online behaviours, leaving them exposed to digital security threats despite having safety protocols in place. Although they implement security checks via antivirus software and other security applications, the respondent highlighted that their focus on thorough data security monitoring and evaluation of the usage of personal devices is limited.

The second subgroup of those adopting a proactive approach to digital security consists of those who rely on external consultants or technical experts to ensure their digital security. In numerous cases, depending solely on an in-house cybersecurity specialist may prove insufficient, as high-risk users might lack the technical resources. Although in-house experts can uphold current security protocols, gaps in knowledge could also greatly impede the organisation's long-term effectiveness. In these circumstances, a highly proficient cybersecurity consultant can provide the expertise to avert potential issues and effectively mitigate security risks.

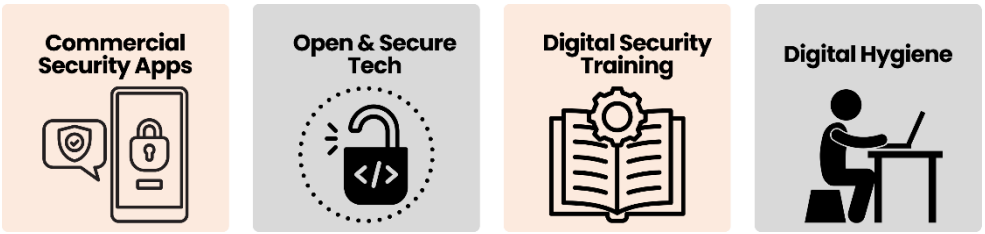
This is a trend that was noted by several respondents. For example, one of them, from Thailand (KII1), mentioned that their organisation outsources these services, partly because assessing institutional-level digital threats and measures presents significant challenges. A respondent from India (KII3) pointed out a trend among local CSOs in India, whereby because of their lack of funding, they rely on

developmental aid and other donor agencies to provide funding to conduct M&E as part of a project they are implementing. This, however, is inconsistent and relies on external agencies to provide the needed support. However, both respondents (KII1; 3) also emphasised that even if these types of services are outsourced, each individual has a certain degree of accountability to keep themselves – and the collective – safe in the digital sphere. This is further elaborated in section 3.3. of the report.

Therefore, as this section has shown, respondents adopt either a reactive or proactive approach to monitor and evaluate digital security threats and assess the most effective digital security measures. The next section delves into the specific measures they have adopted.

3b. Existing Digital Security Measures

In response to the evolving digital security landscape, high-risk users in Asia-Pacific have implemented a variety of tools, technologies, training programs, and protocols to protect themselves and their stakeholders. These measures include using commercial security applications like Virtual Private Networks (VPNs) and Multi-Factor Authentication (MFA) mechanisms, using open and secure technology (OST), creating more opportunities for digital security training, and strengthening individuals' online behaviour. Although these measures are aimed at ensuring a robust digital security framework, there are also remarkable shortcomings that hinder digital security in the region, as will be outlined in section 3.3.



One of the primary measures identified by several respondents is the use of commercial security applications. For instance, several respondents identified the use of antivirus such as Bitdefender (KII2, KII6, KII7), with most using a free or individual licence. Nonetheless, some organisations have purchased enterprise-level antivirus software for their employees, if the budget allows for it (SUR).

The use of VPNs, along with various safety mechanisms, is a standard practice for data protection. For some organisations, VPNs are particularly mandated in contracts or are frequently used when engaging with high-risk individuals or accessing public Wi-Fi, enhancing security during these interactions (KII2, KII3, KII5, KII9, KII12).

Implementing multi-factor authentications is another common measure among high-risk users in the region, adding a layer of security to protect organisational accounts and data (KII5, KII7). A majority of the survey respondents concurred with the use of multi-factor authentications, and to a lesser extent, respondents also described the use of password managers.

For data storage, cloud solutions such as Google Drive and Dropbox are widely employed, offering a reliable means to safeguard sensitive information (KII7, KII8). The use of these file management systems, compared to physical documentation, ensures privacy protections that generally adhere to the higher standards adopted by technology companies like Google (Google, nd.), when compared to offline or storage over self-hosted cloud. Commercial systems like Drive also allow for specific files and folders to be restricted and compartmentalised on a need-to-know basis, preventing a potentially compromised employee account from accessing the entirety of the organisation's files (SUR).

The second set of measures is the adoption and use of open and secure technologies (OSTs) – a measure that is restricted to use by tech-savvy high-risk users and, as a result, less frequently found among the majority of respondents. OST is considered more secure because of the transparency of the source code. With OST, codes undergo public testing and verification to ensure their proper functioning and encryption capabilities (Lynch, 2022). For example, many organisations working on digital rights employ Pretty Good Privacy (PGP) standards for email and file encryption. PGP is a security protocol utilised for both decrypting and encrypting email messages, as well as authenticating email messages through digital signatures and file encryption (Fortinet, 2023). Some (SUR; Asia Centre, 2023) mention the use of OST cloud file management system.

Among the wider range of high-risk users, OSTs have seen popularity for communication. Secure communication applications like Signal and ProtonMail (Asia Centre, 2023) are commonly utilised to ensure private and secure communication (KI10; 12), with special consideration given to using these secure channels when engaging with those from risk-prone countries like Myanmar (KII2) or Vietnam (KII10).

The third set of measures adopted by high-risk users is digital training to empower themselves against digital threats. Digital security experts within organisations provide regular training to their networks, sharing their knowledge and expertise to enhance overall security awareness (KII4; KII12). During periods of heightened threats, some organisations bring in external trainers to strengthen their security measures, ensuring that all staff are up-to-date with the latest security practices (KII9; KII12). Although this type of training does not take place regularly for most participants, some organisations have instituted annual training sessions to continuously update staff on new and emerging security practices, ensuring that the knowledge base remains current and comprehensive (KII10). In many organisations, training covers both the use of digital security applications and tools, as well as M&E training (See section 3.1).

The fourth set of digital security measures identified among respondents is safe and secure digital behaviour online. In addition to technological solutions and training measures, certain habits and protocols are employed to further enhance digital security. Staff are advised against using public internet connections and charging their devices at airports, as these can be vulnerable points of attack (KII3). Regularly deleting chat histories is practised to minimise the risk of sensitive information being compromised (KII5; SUR), while others try to limit their online presence and information provided through social media channels (KII12).

In this regard, many respondents use communication applications which can automate chat deletion. Keeping cameras off during events, disabling microphone access for applications, and avoiding emails from unrecognised addresses are additional safety practices recommended to staff. One organisation (SUR) mentioned that they have developed a Standard Operating Procedure as a manual for their employees to follow in their day-to-day tasks, as well as to handle possible data breaches or other digital security threats.

All in all, these comprehensive digital security measures, including antivirus software, security applications, and encryption protocols, collectively form a robust framework for organisations to protect against a range of digital threats such as malware, hacking, and phishing attacks. They contribute significantly to enhancing overall security posture and safeguarding sensitive information. However, despite their effectiveness, there are notable shortcomings that need to be addressed. These may include gaps in monitoring personal device usage, potential vulnerabilities in existing security protocols, and the need for more proactive measures to stay ahead of evolving cyber threats. Addressing these weaknesses is crucial to maintaining robust digital security practices and mitigating risks effectively.

3c. Strengthening Digital Security Practices

The examination of key informant interviews and survey responses has unveiled significant deficiencies in the digital security practices of high-risk users. These findings underscore critical areas requiring attention and improvement within the realm of digital security.

Making Digital Security a Priority

The overarching issue identified as the key challenge in implementing digital security measures is its lack of prioritisation by public institutions, political parties, INGOs, local CSOs, and individuals alike. Two interlinked factors are key to ensuring the prioritisation of digital security: the creation – or strengthening – of digital security frameworks and increased financial resources.

Regarding digital security frameworks and mechanisms, these are necessary to facilitate the creation and adoption of appropriate measures to respond to digital security threats (KII3). Public institutions and other organisations – including those in the third sector and the media sector – must prioritise bolstering their cybersecurity leadership and governance by appointing experienced cybersecurity professionals to executive roles and board positions. Elevating cybersecurity to the top levels of decision-making promotes a culture of accountability and ensures that security measures receive appropriate attention (Gullapalli, 2023). Promoting professionals to Chief Information Security Officers, endowed with empowerment and a robust mandate, is essential to prioritise strong digital security policies and practices based on prevention (Ibid.).

Prioritising digital security can also ensure that response mechanisms, such as helplines, are in place to address existing digital security threats (KII3), thus avoiding the burden of coping with digital security emergencies solely on individuals or organisations (KII9). Some response mechanisms already exist. For example, Access Now's Digital Security Helpline is a free service for high-risk users facing digital threats. They provide real-time advice to improve online security or offer rapid response assistance in case of attacks. However, while this service can be helpful to many high-risk users globally, users in the Asia-Pacific might not always benefit from it, as it only includes English and Tagalog as widely spoken languages in the region.

The second factor is the allocation of financial resources to develop and implement effective digital security measures (KII2, KII3; KII12). Respondents share the view that the limited prioritisation of digital security among high-risk users is largely due to financial constraints. Cybersecurity measures – particularly those that are robust and advanced, being able to respond to sophisticated attacks with target high-risk individuals and their organisations – are often expensive (KII12), resulting in a lack of, or inadequate protection comparable to the extent of digital security threats they face (KII13). As one respondent from Malaysia noted, "I do not think [digital security] is very high on the priority list, partly because of the cost involved in setting up good cybersecurity measures" (KII2).

Institutional Capacity-building

The prioritisation of digital security and more allocation of financial resources mentioned in the previous section are seen as crucial for another reason: to address the shortage of cybersecurity professionals (KII6; KII13).

It is estimated that the cybersecurity workforce in the Asia-Pacific region has recently reached nearly one million individuals, marking an 11.8% increase from 2022. This growth represents over 100,000 new positions, surpassing the global average growth rate of 8.7%. However, despite reaching its highest recorded workforce in the region, the 2023 ISC2 Cybersecurity Workforce Study reveals that demand continues to outstrip supply. The cybersecurity workforce gap in the region has now risen to a record high, with 2.6 million professionals needed to adequately safeguard digital assets, reflecting a significant 23.4% increase from 2022 (Asia-Pacific Security Magazine, 2023).

A respondent from Cambodia (KII13) provided an insight into how the IT position operates in organisations:

> The IT department is supposed to support the staff, but nowadays, no. It's like a multipurpose position [that includes] photography, videography, video editing, and social media content creation, but they're also responsible for digital security. So even with training to assist the organisation, IT staff struggle to focus on their primary job of supporting staff members because they have too many responsibilities."

This shortage of dedicated personnel and resources further compounds the digital security challenges (KII6), resulting in insufficient support for the maintenance and upgrading of digital security systems, as well as the acquisition of quality security software. Even if some high-risk users and their organisations have the economic means to hire external cybersecurity experts and consultants to evaluate, strengthen, and maintain the standards of their online networks, thus ensuring the digital security of their staff (KII1, 3), not all the strategy should rely solely on their work.

The reliance on external trainers during periods of heightened threats, as mentioned by multiple informants (KII1, KII9; KII13), underscores a potential lack of internal expertise to independently address advanced security challenges, making the strengthening of in-house capabilities imperative to mitigate vulnerabilities effectively.

The pressing shortage of cybersecurity professionals in the Asia-Pacific region highlights a critical need for enhanced digital security since the demand continues to exceed supply. This gap poses significant challenges for maintaining and upgrading digital security systems. Moreover, reliance on external consultants underscores a potential lack of internal expertise to address advanced security challenges independently (KII13). Therefore, prioritising investment in digital security and allocating resources strategically are crucial steps to mitigate vulnerabilities effectively and ensure resilient online environments for organisations and their stakeholders.

Capacity-building Opportunities for Individuals

Although some individuals might think that a one-off digital security training is enough, most respondents who participated in this study emphasised the necessity for more regular and comprehensive training programmes on digital security to adequately equip staff with the knowledge and skills required to effectively handle new and evolving digital threats. While some participants mentioned receiving annual training sessions, they generally felt these were insufficient to instil confidence or provide comprehensive knowledge about digital security (KII1; KII13). A respondent from Pakistan (KII12) validated this point, explaining that, while organisations they partner with may

have allowed staff to undertake digital security training, the evolving nature of threats had quickly made those training outdated. Therefore, as this respondent indicated, periodic training with follow-up sessions is necessary.

Moreover, there was concern that training efforts often targeted technical staff, leaving other personnel, especially those at the managerial level (KII13) uninformed about risks and how to mitigate them (KII7; KII13). While at other times, when digital security training is provided, some participants might complain that the training is not technical enough. This feedback underscores the need for more frequent, inclusive and balanced training initiatives that encompass technical skills and also contribute to raising awareness about the critical importance of digital security, as discussed in section 3.2. Yet, together with calls for increased capacity-building at all levels, a note was also made to strike a balance between the need for continuous learning and adaptation, while ensuring that the information does not overwhelm those who do not have the time dedicated or a strong background in technical issues (KII12).

Incorporating continuous and updated training into the organisation's routine can help ensure that staff remain vigilant and well-informed about the latest security practices and threat landscapes. By doing so, organisations can create a culture of security awareness and proactive behaviour, further strengthening their overall defence against digital threats.

The primary objective of the training, as highlighted by key informants and survey respondents, is to enhance individuals' digital hygiene practices. Digital hygiene encompasses a range of practices aimed at maintaining secure and efficient digital environments. Key aspects include using strong and unique passwords, regularly updating software, and backing up data. Participants emphasised the importance of awareness regarding phishing attacks, adopting secure browsing habits, using antivirus software, and adjusting privacy settings appropriately (Mittal, 2023). Additionally, enabling two-factor authentication and securing devices with PINs or biometrics were noted as crucial steps to bolster security. Key informants also stressed the need for training on effectively protecting digital devices and software with robust measures, as well as on using secure messaging applications like Signal.

Last but not least, in the context of adopting safe digital habits and behaviours, there is a need to increase awareness among high-risk users about their online behaviour when engaging in actions that may seem ostensibly harmless but have real-world risks. This is particularly relevant in countries where state surveillance is highly prevalent, such as Vietnam. Vietnam's Force 47 is a large military unit established in 2017 to manage online discourse. With potentially thousands of members, the unit combats online criticism of the government by promoting pro-government views and reporting opposing content. This approach has raised concerns about online harassment and the manipulation of social media platforms (Dien Nguyen, 2021; Pearson, 2021).

In this context, adopting strong online security measures is essential not only for high-risk users' digital safety but also for their offline security. The views that a respondent from Vietnam (KII5) shared show the need to promote safe digital habits, particularly in politically sensitive environments. Using the Force 47 example, this respondent explained how even simple actions like liking a Facebook page can significantly impact safety offline.

> In our organisation, we discourage staff from liking our posts or politically sensitive content because it can expose them to potential dangers. In Vietnam, there is a cyber security unit known as Force 47, which consists of about 10,000 individuals dedicated to monitoring online activities. They track people who engage with political posts, compiling lists of individuals who exhibit such behaviours. Those on these lists can be arrested if their online habits raise too many red flags (KII5).

This respondent also shared a case involving one of their team members who frequently posted political and social content online. Despite these posts not being related to their organisation, the individual was summoned for interrogation and detained for 17 days. The authorities had detailed records of his online activities, including comments, likes, and group memberships on Facebook, as they had been monitoring the individual and tracking every online action. This example underscores the importance of being vigilant about online behaviour. Ensuring robust online security practices can protect high-risk users from potential offline repercussions.

The data collected from the survey, which was designed to gather primary data, indicates specific areas where respondents would like to receive more training. Table 5 shows the percentage of respondents that selected each of the options of a provided list of options.

Table 3: Priority Digital Security Training Topics

Topic	Share
Training on mobile device security	54.41%
Training on protecting personal and company data	45.59%
Training on relevant laws and surveillance measures adopted by different actors	35.29%
Training on recognising and navigating online hate speech and disinformation	33.82%
Training on how to respond to a security breach	30.88%
Training on understanding and using digital protection keys (e.g., security tokens)	30.88%
Training on safe internet browsing habits	29.41%
Training on using security software effectively	19.12%
Training on creating strong passwords	11.76%
Training on recognising phishing emails and scams	7.35%

With regards to the implementation of the training, informants highlighted the need for a comprehensive set of best practices documents, training resources and manuals. For instance, best practice documents, continually updated, should be developed and encompass a range of measures, including encryption, secure communication protocols, and digital hygiene. By adhering to these guidelines, individuals can better protect their sensitive information and evade surveillance efforts (KII1). Case studies from organisations like Access Now and the Electronic Frontier Foundation demonstrate the efficacy of these practices in safeguarding activists and journalists in repressive environments.

Furthermore, curricula and resources for capacity-building activities play a pivotal role in guiding and streamlining digital security training sessions to best impart high-risk users with the knowledge and skills needed to defend against digital threats. The example of the Southeast Asia Freedom of Expression Network (SAFEnet) illustrates how capacity-building initiatives can bolster the resilience of vulnerable communities against online attacks. Its training on digital security, using a curriculum developed based on research, effectively addresses key digital security challenges faced by vulnerable communities (Anang, 2023).

Another example of a capacity-building initiative includes a series of online training programs aimed at the public sector to enhance protection against digital security risks (GovInsider, 2017). These training sessions are designed to equip government officials and agencies with the necessary skills and knowledge to mitigate cyber threats effectively. By focusing on the specific needs and vulnerabilities of public sector entities, such as government offices and agencies, these training programs aim to bolster their resilience against various forms of digital security challenges, including cyberattacks, data breaches, and online surveillance.

It must also be noted that addressing the complex digital security challenges in the Asia-Pacific necessitates collaborative efforts between various stakeholders, including civil society organisations, tech companies, and governments. By fostering partnerships and sharing expertise, stakeholders can develop more robust and context-specific best practices tailored to the region's unique challenges.

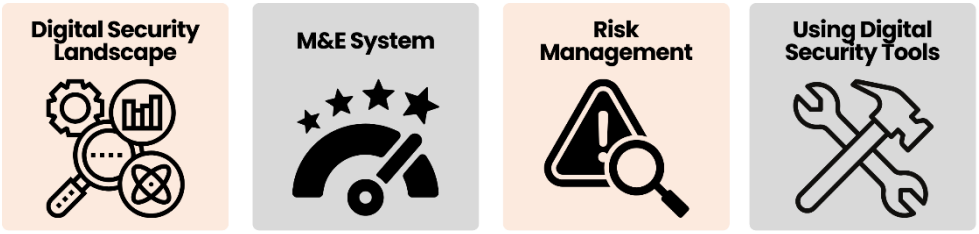
Initiatives such as the Digital Security Exchange play a crucial role in facilitating collaboration by linking high-risk users with digital security experts and resources. It serves as a platform where individuals and organisations facing digital threats can access technical assistance, training programmes, and guidance on improving their digital security measures. By connecting these high-risk users with experts who understand the unique challenges they face, Digital Security Exchange helped strengthen their resilience against cyber threats. This collaborative approach not only enhanced the digital security capabilities of vulnerable groups but also promoted a community-driven effort to safeguard digital spaces and protect high-risk users.

At the regional level, initiatives such as the Association of Southeast Asian Nations' (ASEAN's) cybersecurity strategy (2022) indicate a growing emphasis on protecting public institutions from digital security threats. This strategy underscores the importance of regional cooperation in addressing cyber threats that target governmental bodies and critical infrastructure across Southeast Asia. By promoting collaboration among member states, ASEAN aims to enhance cybersecurity capabilities, share threat intelligence, and develop common frameworks for cyber defence. This approach not only strengthens individual member states' resilience to cyber-attacks but also fosters a unified response to evolving digital threats in the region.

All in all, the insights gleaned from key informant interviews highlight several shortcomings in current digital security practices among high-risk users. These findings underscore the urgent need for improved resource allocation, enhanced internal capacity, and comprehensive training programmes to bolster digital security resilience and mitigate risks effectively. Addressing these deficiencies is paramount to safeguarding the integrity and confidentiality of organisational data in an increasingly complex and dynamic digital landscape.

4. Recommendations

The output of this report is two-fold. First, it has shown that, alongside numerous opportunities, the popularisation of digital tools and media has led to increased digital threats, especially for those working on sensitive topics or with confidential information, identified as high-risk users. Second, it has demonstrated that while many of these high-risk users have adopted some digital security measures, there is a pressing need to strengthen and regularise digital security training to ensure they can operate effectively and safely online. Based on the findings of this report, this section provides the following recommendations to enhance digital security training.



To **strengthen the understanding of the digital security landscape,** digital security training should:

- Adjust the content of the training to consider the specific contextual settings in which they are conducted by emphasising how socio-political contexts influence each digital security landscape, thus clarifying why certain groups or sectors are targeted more frequently.
- Focus on the specific impact of digital security threats on high-risk users – as opposed to internet users as a whole. Tailor the training to address the unique challenges faced by high-risk users.
- Emphasise the inclusion of case studies relevant to the region, country and profile of the trainees, ensuring that these examples resonate with the trainees' experiences and contexts.

To i**mprove the effectiveness of monitoring and evaluation systems,** digital security training should:

- Emphasise the critical benefits of proactive digital security monitoring and evaluation. Highlight how early identification of vulnerabilities can prevent exploitation, thereby effectively mitigating risks and enhancing overall security.
- Include comprehensive guidance on setting up a structured M&E framework. This should include:
    - Conducting digital security vulnerability assessments regularly and thoroughly to identify and address weaknesses with regard to digital security protection
    - Implementing advanced threat detection systems to continuously monitor and detect potential digital security threats.
    - Establishing regular training programmes and providing educational resources for employees to ensure all personnel are equipped with the ability to recognise, report on, and respond to, potential digital security threats.
- Emphasise the importance of regularly updating the M&E framework to stay aligned with evolving threats and emerging security technologies by encouraging a dynamic approach to M&E that adapts to new challenges and incorporates the latest advancements in digital security.

- Provide examples of best practices from successful M&E implementations and offer a template of a digital security M&E framework. These resources should serve as starting points for trainees to customise according to the specific needs of their organisation.

To **strengthen the capacity of users to manage digital security risks,** digital security training should:

- Highlight the importance of protecting personal and organisational information in these environments by providing detailed guidelines on using secure communication tools and maintaining privacy, especially in politically sensitive contexts. Also covers essential digital hygiene practices, threat awareness and incident response protocols.
- Equip trainees with practical knowledge to recognise and counter phishing attacks and other prevalent digital security threats specific to their sector or region. Training should focus on:
    - Common social engineering tactics – which aim to manipulate victims into sharing information – and how to defend against them.
    - Techniques for identifying suspicious emails, messages and websites to detect phishing attempts and malicious content.
    - Ensure these programs are inclusive, addressing the needs of diverse roles of high-risk users.

To **strengthen the effective utilisation of tools to strengthen digital security,** digital security training should:

- Train on the importance of using reputable antivirus software, VPNs, multi-factor authentication (MFA), password managers, and other endpoint security tools to safeguard users against various digital security threats and enhance overall security.
- Stress the advantages of adopting open and secure technologies (OST) in workflows and systems.
    - Highlight the benefits of source code transparency, as open-source solutions allow for greater visibility and auditing of its systems.
    - Emphasise the advantages of community-driven development, where the collaborative nature of open-source projects leads to the rapid identification and resolution of security issues. Furthermore, the community can suggest features that would enhance their productivity and effectiveness.
    - Underscore strong security standards that are often incorporated in open-source solutions.
- Deliver specialised training sessions focusing on security keys to emphasise their importance and implementation for enhanced protection of high-risk users. These sessions should highlight how physical security keys enhance protection against hacking and credential theft.
- Conduct training sessions focused on effective strategies and tools for defending websites against Distributed Denial of Service (DDoS) attacks. Cover topics such as:
    - Identifying which websites are at risk during politically sensitive periods by evaluating their key functions, assessing previous incidents (or similar incidents in other regions), and understanding the target audience of the website.
    - Best practices to mitigate the risk of DDoS attacks and preventative measures such as tools and services to protect against DDoS attacks.
    - Steps to minimise the impact of an attack and recover operations, including backup systems and post-attack assessments to strengthen defences.

5. Conclusion

Amidst the rapid expansion of internet and digital technology in the Asia-Pacific, rising threats like cyberattacks, data breaches, and doxxing undermine privacy and institutional integrity. These challenges, particularly affecting high-risk users such as public officials and rights defenders, highlight the critical need for robust digital security measures.

To address these issues, strengthening digital security practices and policies is essential for fostering a secure digital environment that supports regional stability and growth. Increasing digital security training for high-risk users is crucial to equipping them with the tools and knowledge needed for digital safety. This report emphasises four key areas in digital security training to ensure comprehensive protection against evolving threats.

Firstly, digital security training programmes should be tailored to the specific contextual settings and socio-political environments in which they are implemented. This approach not only helps high-risk users understand why they are targeted but also provides them with relevant strategies to mitigate these risks. By emphasising the socio-political contexts influencing digital security landscapes, training can offer more nuanced and effective guidance. Additionally, incorporating region-specific case studies will ensure the training resonates with the trainees' experiences, making it more practical and impactful.

Secondly, capacity-building efforts should focus on enhancing monitoring and evaluation (M&E) systems. This involves establishing M&E frameworks with regular vulnerability assessments, advanced threat detection systems, and continuous training programmes. Regular updates are crucial to stay aligned with evolving threats and technologies. Proactive monitoring can prevent exploitation by identifying vulnerabilities early, thus enhancing overall security. Providing best practice examples and templates will help trainees customise frameworks to their organisational needs.

Thirdly, training should equip high-risk users with practical skills to manage digital security risks effectively. This includes guidelines on secure communication, privacy in politically sensitive contexts, and essential digital hygiene. Trainees should be well-versed in threat awareness and incident response protocols. The training should also focus on recognising and countering phishing attacks and other sector-specific threats. By addressing common social engineering tactics and techniques for identifying suspicious emails, messages, and websites, the training can enhance users' ability to defend against malicious content.

Lastly, prioritising tools like antivirus software, VPNs, MFA, password managers, and other endpoint security tools is crucial for enhancing overall security. Training should promote the adoption of open and secure technologies (OST) in workflows, highlighting benefits such as source code transparency and community-driven development. Specialised sessions on security keys should emphasise their effectiveness against hacking and credential theft. Additionally, training on defending against DDoS attacks should cover identifying vulnerable websites, implementing best practices, and establishing recovery procedures, ensuring high-risk users can effectively manage digital security threats.

As the digital sphere evolves rapidly, its expected that upgraded threats from targeted phishing, ransomware attacks and cyber extortion, the Internet of Things (IoT), cloud technology, quantum computing, and artificial intelligence (AI) require vigilance and monitoring. Digital security training must factor in the outcomes of this rapid evolution in technology so that high-risk users can be inoculated from latest threats and vulnerabilities, thereby strengthening their online safety moving forward.

Phishing is expected to evolve by becoming more personalised and targeted, using sophisticated social engineering tactics to deceive victims. Attackers may gather detailed information about their

targets from social media or other online sources, making phishing emails appear more legitimate and harder to detect. Additionally, advances in AI may enable attackers to generate highly convincing messages that mimic the style of trusted contacts or organisations.

Ransomware, similarly, is predicted to grow more complex, employing advanced encryption methods and even targeting critical infrastructure. Attackers may also use double extortion tactics, where they not only lock files but also threaten to release sensitive data, making the consequences of such attacks even more severe and driving up the number of successful extortion cases.

As individuals increasingly rely on the IoT to simplify daily tasks, their exposure to online threats grows due to the expanding number of connected devices. Each smart device, such as smartwatches or internet-connected cars, introduces additional entry points for cyberattacks. Hackers can exploit vulnerabilities in these devices' software or weak security configurations to gain access to personal data or networks. Furthermore, insecure IoT devices might also be used as part of larger botnet attacks, amplifying the potential scale of cyber threats across interconnected systems. Therefore, each new device increases the overall risk to security and privacy.

Similarly, organisations and individuals who plan to rely heavily on cloud technology to enhance their efficiency and effectiveness will also be exposed to increased cyberattack risks. This is because cloud storage centralises large volumes of sensitive data, making it a target for hackers. If cloud services are not configured with strong security measures like encryption or multi-factor authentication, vulnerabilities in access controls can be exploited. Furthermore, the reliance on third-party service providers for cloud infrastructure means that any security weaknesses or breaches within those providers' systems could potentially compromise the data. Lastly, as data is transferred to and from the cloud, insecure network connections can be exploited, leading to potential data interception or theft.

To protect users, quantum computing will play a key role in protecting users by enhancing computational power, enabling the development of more sophisticated encryption methods and cybersecurity tools that can better detect and respond to threats in real time. For example, quantum encryption techniques like quantum key distribution could make it nearly impossible for hackers to intercept communications without being detected. However, this same computational power could also be exploited by hackers to break current encryption standards. Quantum algorithms may allow attackers to solve complex cryptographic problems much faster, rendering traditional encryption methods vulnerable to breaches. As a result, both defensive and offensive capabilities in cybersecurity will evolve in tandem.

Lastly, the advancement of AI will have a growing impact on digital security. AI has the potential to both intensify existing threats – such as the creation of deepfakes that impersonate public figures – and provide solutions to enhance security measures. AI-powered tools can improve threat detection, automate incident responses, and offer advanced analytics to anticipate and counteract potential breaches.

Implementing the recommendations from this report will be a crucial first step for any organisation or individuals planning to roll out digital security training. In this way, training providers can enhance the capacity of high-risk users to effectively protect themselves against digital threats. Thereafter, a proactive approach with an eye on upcoming technological developments and their impact on digital threats is essential for future oriented training aimed at safeguarding sensitive information and maintaining operational integrity.

BIBLIOGRAPHY

Adair, Stephanie (2023) 'TikTok sweeps wave of change over Thailand's election campaigns', The Nation, at: https://www.nationthailand.com/thailand/politics/40028083.

AFP (2022) 'South Korea's cyberbullies driving victims to suicide', The Phnom Penh Post, at: https://www.phnompenhpost.com/lifestyle/south-koreas-cyberbullies-driving-victims-suicide.

Aljazeera (2024) 'China-backed hackers stepping up attacks on Taiwan, cybersecurity firm says', Aljazeera, at: https://www.aljazeera.com/economy/2024/6/24/china-backed-hackers-stepping-up-attacks-on-taiwan-cybersecurity-firm-says.

Aljazeera (2024) 'Sri Lanka Parliament passes bill to regulate online content', Aljazeera, at: https://www.aljazeera.com/news/2024/1/24/sri-lanka-parliament-passes-bill-to-regulate-online-content.

ANANG (2023) 'SAFEnet provides digital security training for critical groups in South Kalimantan', Indonesia Today, at: https://indonesiatoday.co/safenet-provides-digital-security-training-for-critical-groups-in-south-kalimantan.

AP News (2024) 'Spain reopens a probe into a Pegasus spyware case after a French request to work together', AP News, at: https://apnews.com/article/spain-france-spyware-pegasus-49fd974eb9245d4a87361bde3001542b.

ASEAN (2022) *ASEAN Cybersecurity Cooperation Strategy (2021–2025)*, ASEAN Secretariat, at: https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.

Asia Centre (2023) Digital Security & Human Rights Defenders Landscape: Recommendations for NHRIs in the Asia-Pacific, Bangkok, Thailand: Asia Centre and Asia-Pacific Forum, at: https://asiacentre.org/wp-content/uploads/Digital-Security-Human-Rights-Defenders-Landscape-Recommendations-for-NHRIs-in-the-Asia-Pacific.pdf.

Asia Centre (2023) *Digital Security and Human Rights Defenders in the Asia-Pacific*, Bangkok, Thailand: Asia Centre and EngageMedia, at: https://asiacentre.org/wp-content/uploads/Digital-Security-and-Human-Rights-Defenders-in-the-Asia-Pacific.pdf.

Asia Centre (2023) *State-sponsored Online Disinformation: Impact on Electoral Integrity in Thailand*, Bangkok, Thailand: Asia Centre, at: https://asiacentre.org/wp-content/uploads/Digital-Security-and-Human-Rights-Defenders-in-the-Asia-Pacific.pdf.

Asia-Pacific Security Magazine (2023) 'Gap of 2.6 million cybersecurity professionals looms', Asia-Pacific Security Magazine, at: https://www.asiapacificsecuritymagazine.com/gap-of-2-6-million-cybersecurity-professionals-looms.

Bopha Phorn & Shaun Turton (2021) 'Cambodia's prime minister is Zoombombing opposition meetings', Rest of World, at: https://restofworld.org/2021/cambodia-pm-zoom-calls.

Borowiec, Steven (2020) 'How South Korea's nightclub outbreak is shining an unwelcome spotlight on the LGBTQ community', The Time, at: https://time.com/5836699/south-korea-coronavirus-lgbtq-itaewon.

Bunnag, Nad (2024) 'It's not our fault for being born female – Chonthicha Jangrew, Move Forward Party MP', Thai PBS World, at: https://www.thaipbsworld.com/its-not-our-fault-for-being-born-female-chonthicha-jaengrew-move-forward-party-mp.

CenterLaw Philippines (nd.) 'About', CenterLaw Philippines, at: https://centerlawph.org/about.

Cheung, Eric (2023) 'Taiwan faces a flood of disinformation from China ahead of crucial election. Here's how it's fighting back', CNN, at: https://edition.cnn.com/2023/12/15/asia/taiwan-election-disinformation-china-technology-intl-hnk/index.html.

Chiu, Ethan (2023) 'Analysing Taiwan's readiness and response to PRC offensive cyber operations', The Yale Review of International Studies, at: https://yris.yira.org/column/analyzing-taiwans-readiness-and-response-to-prc-offensive-cyber-operations.

Chong, Terrence, Carmen Leong, Shan L Pan Shamshul Bahri & Ali Fauzi Ahmad Khan (2014) 'Use of Social Media in Disaster Relief Duting the Kuantan (Malaysia) Flood', paper presented at the 35th International Conference on Information Systems, Auckland, New Zealand, at: https://core.ac.uk/download/pdf/162014173.pdf.

CNA (2023) 'Kenneth Jeyaretnam given sixth POFMA order over Ridout Road comments', CNA, at: https://www.channelnewsasia.com/singapore/kenneth-jeyaretnam-sixth-pofma-order-correction-direction-gutzy-toc-ridout-road-4132636.

Congjuico, Teresa S. (2014) 'Social Media for Risk Management and Emergency Response for Philippine Local Government Units', *Journal of Management and Development Studies* 3: 20–38, at: https://jmds.upou.edu.ph/index.php/journal/article/view/7/7.

Davison, Catherine (2022) 'Nepal's early-warning system reduces flood fatalities', DW, at: https://www.dw.com/en/nepals-early-warning-system-reduces-flood-fatalities/a-62981276.

Dien Nguyen An Luong (2022) 'How the Vietnamese state uses cyber troops to shape online discourse', ISEAS Perspectives, at: https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2021-22-how-the-vietnamese-state-uses-cyber-troops-to-shape-online-discourse-by-dien-nguyen-an-luong.

Economy Next (2021) 'Sri Lanka cabinet nod for laws against "false propaganda" online', Economy Next, at: https://economynext.com/sri-lanka-cabinet-nod-for-laws-against-false-propaganda-online-80943.

Ellis-Petersen, Hannah (2023) 'Could trouble for Adani trip up Narendra Modi?', The Guardian, at: https://www.theguardian.com/business/2023/feb/15/could-trouble-for-adani-trip-up-narendra-modi.

Fortinet (2023) 'What is PGP? Pretty Good Privacy definition', Fortinet, at: https://www.fortinet.com/resources/cyberglossary/pgp-encryption.

Foyez, Ahammad (2021) 'Bangladesh ruling party mobilises online propaganda army to target next election', Benar News, at: https://www.benarnews.org/english/news/bengali/bangladesh-government-online-activists-09142021133831.html.

Gallo, William & Lee Juhyun (2021) 'South Korea fights "fake news", but critics claim it's gagging the press', VOA News, at: https://www.voanews.com/a/east-asia-pacific_south-korea-fights-fake-news-critics-claim-its-gagging-press/6219375.html.

Gitzen, Timothy (2020) 'Tracing homophobia in South Korea's coronavirus surveillance program', The Conversation, at: https://theconversation.com/tracing-homophobia-in-south-koreas-coronavirus-surveillance-program-139428.

Gitzen, Timothy & Wonkeun Chun (2021) 'Pandemic Surveillance and Homophobia in South Korea', Social Science Research Council, at: https://items.ssrc.org/covid-19-and-the-social-sciences/covid-19-fieldnotes/pandemic-surveillance-and-homophobia-in-south-korea.

Google (nd.) 'How Drive protects your privacy & keeps you in control', Google, at: https://support.google.com/drive/answer/10375054?hl=en.

GovInsider (2017) 'New online cyber security skills series launched for officials in Asia', GovInsider, at: https://govinsider.asia/intl-en/article/new-online-cyber-security-skills-series-launched-for-officials-in-asia.

Gullapalli, Vivek (2023) 'Why is the Asia-Pacific region a target for cybercrime - and what can be done about it?', World Economic Forum, at: https://www.weforum.org/agenda/2023/06/asia-pacific-region-the-new-ground-zero-cybercrime.

Han, Kirsten. (2024) 'POFMA Tracker'. LinkedIn. August 2024. Available at: https://www.linkedin.com/posts/kirsten-han-3466a8230_its-ticked-past-midnight-in-singapore-now-activity-7207778953103618048-K3LQ/

Hashim, Asad (2017) 'Pakistan: Zafar Achakzai charged for anti-army post', Aljazeera, at: https://www.aljazeera.com/news/2017/6/30/pakistan-zafar-achakzai-charged-for-anti-army-post.

Huang, Elaine (2022) 'Despite ban, Chinese surveillance equipment infiltrating Taiwan in plain sight', Commonwealth Magazine, at: https://english.cw.com.tw/article/article.action?id=3301.

Human Rights Commission of Pakistan (nd.) 'Campaigns', Human Rights Commission of Pakistan, at: https://hrcp-web.org/hrcpweb/campaigns.

Hynes, Mike (2021), 'Online Privacy and Surveillance', *The Social, Cultural and Environmental Costs of Hyper-Connectivity: Sleeping Through the Revolution*, Leeds, UK: Emerald Publishing, DOI:10.1108/978-1-83909-976-220211006.

iLaw (2024) 'Parasite that Smiles: Pegasus Spyware Targeting Dissidents in Thailand', iLaw, at: https://www.ilaw.or.th/wp-content/uploads/2024/04/Pegasus-Spyware-Targeting-Dissidents-in-Thailand.pdf.

Infoxchange & Tech Soup Asia-Pacific (2023) 'Asia-Pacific NGO Digital Capability Report 2023', NGO Digital Transformation, at: https://digitaltransformation.ngo/sites/default/files/IX_APACReport23.pdf.

Iwaniuk, Jakub (2024) 'Pegasus probe in Poland reveals unprecedented use of spyware by previous government', Le Monde, at: https://www.lemonde.fr/en/international/article/2024/03/04/pegasus-probe-in-poland-reveals-unprecedented-use-of-spyware-by-previous-government_6584086_4.html.

Kaspersky (nd.) 'What is doxing – definition and explanation', Kaspersky, at: https://www.kaspersky.com/resource-center/definitions/what-is-doxing.

Kaspersky (nd.) 'What is zero-click malware, and how do zero-click attacks work?', Kaspersky, at: https://usa.kaspersky.com/resource-center/definitions/what-is-zero-click-malware.

Kemp, Simon (2024) 'Digital 2024', Datareportal, https://datareportal.com/reports.

Kim Min Joo & Michelle Ye Hee Lee (2022) 'Ahead of election, South Korea's feminists battle sexist backlash', Washington Post, at: https://www.washingtonpost.com/world/2022/03/05/south-korea-gender-wars.

Klingová, Katarína (2023) 'Information Operations', The Foundation for European Progressive Studies, at: https://feps-europe.eu/wp-content/uploads/2023/01/13.-Information-operations-by-Katarina-Klingova.pdf.

Köckritz, Angela (2023) 'In a savvy disinformation offensive, China takes aim at Taiwan election', Mercator Institute for China Studies (MERICS), at: https://merics.org/en/report/savvy-disinformation-offensive-china-takes-aim-taiwan-election.

Kwentong San Andres (nd.) main webpage, CentreLaw, at: https://kwentong-san-andres-microsite.webflow.io.

Kyodo News (2020) 'Abe under fire after prosecutor seen close to him quits for gambling', Kyodo News, at: https://english.kyodonews.net/news/2020/05/d7d113891997-breaking-news-cabinet-approves-prosecutor-kurokawas-resignation-over-gambling.html.

Lamb, Kate & Fanny Potkin (2021) 'Indonesian anti-graft activists complain of digital attacks', Reuters, at: https://www.reuters.com/technology/indonesian-anti-graft-activists-complain-digital-attacks-2021-05-25.

Lane, Max (2021) 'The KPK controversy keeps corruption a central issue in public consciousness', Fulcrum, at: https://fulcrum.sg/the-kpk-controversy-keeps-corruption-a-central-issue-in-public-consciousness.

Lau, Stuart (2024) 'China bombards Taiwan with fake news ahead of election', Politico, at: https://www.politico.eu/article/china-bombards-taiwan-with-fake-news-ahead-of-election.

Lynch, Jim (2015) 'Why is open source software more secure?', InfoWorld, at: https://www.infoworld.com/article/2985242/why-is-open-source-software-more-secure.html.

Mahmud, Faisal (2021) 'Bangladesh's ruling party to unleash online army to "stifle" opposition', TRT World, at: https://www.trtworld.com/magazine/bangladesh-s-ruling-party-to-unleash-online-army-to-stifle-opposition-50130.

Media Advocacy Group (2022) 'Online Violence against Women Journalists: Study Brief', Media Advocacy Group, at: https://mag.org.np/wp-content/uploads/2022/12/Online-Violence-and-Harassment-Against-Women-English.pdf.

Mittal, Ayush (2023) 'What is digital hygiene? And ways to hide your online activity', Medium, at: https://medium.com/@sprayiton1122/what-is-digital-hygiene-and-ways-to-hide-your-online-activity-554ee7ebad3e.

Naik, Raqib Hameed (2021) 'Students in India use social media to fight coal projects', Earthbeat, at: https://www.ncronline.org/earthbeat/justice/students-india-use-social-media-fight-coal-projects.

Nam, Jimin (2024) 'Understanding antifeminist backlash in the South Korean context: Remnants of militarism and patriarchy', 9DashLine, at: https://www.9dashline.com/article/understanding-antifeminist-backlash-in-the-south-korean-context-remnants-of-militarism-and-patriarchy.

Nelson, Nate (2024) 'Bangladeshi elections come into DDoS Crosshairs', Dark Reading https://www.darkreading.com/ics-ot-security/bangladeshi-elections-ddos-crosshairs.

Nepal Press Freedom (2020) 'Journalist Binu Subedi bullied online for criticising government actions', Nepal Press Freedom, at: https://nepalpressfreedom.org/main/issue-single/1175.

Nguyen, Jason (2022) 'Vietnam's surveillance state: Following China's model of digital authoritarianism?', The Vietnamese, at: https://www.thevietnamese.org/2022/08/vietnams-surveillance-state-following-chinas-model-of-digital-authoritarianism.

Paulger, Dominic (2022) 'Japan: Status of Consent for Processing Personal Data', Future of Privacy Forum, at: https://fpf.org/wp-content/uploads/2022/09/ABLI-FPF-Consent-Project-Japan-Jurisdiction-Report.pdf.

PDC Global (2020) 'Philippines project gets boost from new social media platform for humanitarian response', PDC Global, at: https://www.pdc.org/philippines-project-social-media.

Pearson, James (2021) 'Insight: How Vietnam's "influencer" army wages information warfare on Facebook', Reuters, at: https://www.reuters.com/world/asia-pacific/how-vietnams-influencer-army-wages-information-warfare-facebook-2021-07-09.

Positive Technologies (2023) *Cybersecurity Threatscape Asia 2022-2023*, Positive Technologies, at: https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cybersecurity-threatscape-Asia-2022-2023-en.pdf.

PRODRAFT (2023) 'Proactive vs. reactive approach to cybersecurity: Why timely detection matters', PRODRAFT, at: https://resources.prodaft.com/prodaft-threat-intelligence-blog/proactive-vs-reactive-approach-to-cybersecurity-and-why-it-matters.

Raaban, Mohamad Razali & Mokhtar Muhammad (2023) 'The Role of Social Media In Increasing Political Influence For Malay Politicians', *Asian Journal of Research in Education and Social Sciences* 5(2): 178–185, at: https://myjms.mohe.gov.my/index.php/ajress/article/view/22226.

Rajapakse, Chiranthi (2023) 'Sri Lanka's new Bill on Online Safety: Comparison with Singapore', LIRNEasia, at: https://lirneasia.net/2023/09/sri-lanka-online-safety-bill.

Reuters (2024) 'India's Adani gets top court relief on further probe over Hindenburg report', Aljazeera, at: https://www.aljazeera.com/news/2024/1/3/indias-adani-wins-top-court-relief-on-further-probe-over-hindenburg-report.

Rina Chandran (2022) 'Activists say China's new Silk Road equips autocrats with spy tech', Context, at: https://www.context.news/surveillance/activists-say-chinas-new-silk-road-equips-autocrats-with-spy-tech.

Roengtam, Sataporn (2017) 'Social Media Use and Citizen Engagement in Local Government of Thailand', in Vito Bobek (ed.) *Management of Cities and Regions*, Rijeka, Croatia: Intechopen, DOI:10.5772/intechopen.70982.

Saaliq, Shiekh (2023) 'Indian police arrest a news site's editor and administrator after raiding homes of journalists', AP News, at: https://apnews.com/article/india-press-freedom-newsclick-arrest-raid-3faa0830e9f3bcd4e75f1b7df404f432.

Saeed, Aamir (2024) 'Pakistan launches special cybercrime unit under controversial PECA law, shifts role from FIA', Arab News, at: https://www.arabnews.pk/node/2504136/pakistan.

Sangfor Technologies (2023) 'Comparing proactive vs. reactive cybersecurity in 2023', Sangfor Technologies, at: https://www.sangfor.com/blog/cybersecurity/proactive-vs-reactive-cybersecurity-2023.

Scott-Railton, John, Bill Marczak, Irene Poetranto, Bahr Abdul Razzak, Sutawan Chanprasert & Ron Deibert (2022) 'GeckoSpy: Pegasus Spyware Used against Thailand's Pro-Democracy Movement', The Citizen Lab, at: https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement.

Seldin, Jeff (2024) 'Cyber-attacks spike suddenly prior to Taiwan's election', VOA News, at: https://www.voanews.com/a/cyber-attacks-spike-suddenly-prior-to-taiwan-s-election-/7485386.html.

Shahid, Jamal (2018) 'Twitter threatened with shutdown in Pakistan', Dawn, at: https://www.dawn.com/news/1427274.

Singh, Shivam Shankar (2019) 'A former BJP data analyst reveals how the party's WhatsApp groups work', Quartz, at: https://qz.com/india/1553765/bjps-whatsapp-ops-is-what-cambridge-analytica-can-only-dream-of.

Suphasan, Non (2021) 'ตัวตลกอันตราย: กองทัพมินเนี่ยนปกป้องสถาบัน และการเคลื่อนไหวโต้กลับที่เฉิ่มเชย น่าขำขัน แต่ไปด้วยกันได้ดีกับอำนาจรัฐ *[Dangerous clowns: The monarchy-protecting Minion Army and a dull and laughable counter-movement that goes hand in hand with state power]*', Prachatai, at: https://prachatai.com/journal/2021/06/93614.

The Business Times (2023) 'TikTok advantage behind Move Forward Party's big win in Thailand election', The Business Times, at: https://www.businesstimes.com.sg/international/tiktok-advantage-behind-move-forward-partys-big-win-thailand-election.

The Economic Times (2024) 'WhatsApp, social media influencers emerge as go to campaign mediums as parties sound poll bugle', The Economic Times, at: https://economictimes.indiatimes.com/tech/technology/whatsapp-social-media-influencers-emerge-as-go-to-campaign-mediums-as-parties-sound-poll-bugle/articleshow/108557477.cms.

The Human Rights Campaign (2017) 'HRC outraged at Bangladesh arrests, outing of 28 men', The Human Rights Campaign, at: https://www.hrc.org/news/hrc-outraged-at-bangladesh-arrests-outing-of-28-men.

The Jakarta Post (2024) 'KPU websites face "extraordinary" cyberattacks on voting day', The Jakarta Post, at: https://www.thejakartapost.com/indonesia/2024/02/15/kpu-websites-face-extraordinary-cyberattacks-on-voting-day.html.

The Times of India (2022) 'BJP first to recognise social media as the new elector', The Times of India, at: https://timesofindia.indiatimes.com/india/bjp-first-to-recognise-social-media-as-the-new-electoral-battlefield/articleshow/94596087.cms.

Trisuwan, Hathaikan (2020) 'ราษฎร 2563: ลูกเกด ชลธิชา แจ้งเร็ว อดีตผู้ถูกจองจำ-ผู้เจรจากับ ตร.-ผู้ถูกไลให้เปลี่ยนนามสกุล *[Ratsadon 2020: Lukket Chonticha Jandrew, ex-prisoner - negotiator with the Police - a person forced to change last name]*', BBC Thai, at: https://www.bbc.com/thai/thailand-54758289.

UCA News (2023) ' LGBTQI+ meet shifted out of Indonesian capital after death threats', UCA News, at: https://www.ucanews.com/news/lgbt-meet-shifted-out-of-indonesian-capital-after-death-threats/101987.

Uchida Atsuhiko (2023) 'Participation Through Social Media by Japanese Youth', *Kyoto Review of Southeast Asia* 36, at: https://kyotoreview.org/issue-36/political-participation-through-social-media-by-japanese-youth.

VOA News (2023) 'Journalists, government critics in India targeted with Pegasus Spyware', VOA News, at: https://www.voanews.com/a/journalists-government-critics-in-india-targeted-with-pegasus-spyware/7416268.html.

Yamamoto Kayoko (2021) 'Utilization of Social Media at the Times of Natural Disasters in Japan', paper presented at the International Conference on ICT Enhanced Social Sciences and Humanities 2021, DOI:10.21428/7a45813f.86f0b6ac.

Yang, Zeyi (2024a) 'Why Threads is suddenly popular in Taiwan', MIT Technology Review, at: https://www.technologyreview.com/2024/04/02/1090518/threads-taiwan-election-politics-popular.

Yang, Zeyi (2024b) 'Threads is giving Taiwanese users a safe space to talk about politics', MIT Technology Review, at: https://www.technologyreview.com/2024/04/03/1090601/threads-taiwanese-users-talk-politics.

"Act on the Protection of Personal Information" (2003), Cabinet Secretariat of Japan, at: https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf.

"Prevention of Electronic Crimes Act" (2016), National Assembly of Pakistan, at: https://www.na.gov.pk/uploads/documents/1462252100_756.pdf.

"Protection from Online Falsehoods and Manipulation Act" (2019), Singapore Statutes Online, at: https://sso.agc.gov.sg/Act/POFMA2019.

ANNEX

Profiles of Key Informants

Code	Country	Key Informant Profile	Date of Interview
KII1	Thailand	Legal advocate	19 April 2024
KII2	Malaysia	Communications professional	22 April 2024
KII3	India	Representative of an INGO	22 April 2024
KII4	Indonesia	Representative of an organisation working on digital rights	24 April 2024
KII5	Vietnam	Representative of a diaspora NGO	25 April 2024
KII6	Nepal	Representative of an organisation working on digital rights	26 April 2024
KII7	Japan	Representative of a nationally-based NGO	2 May 2024
KII8	South Korea	Independent academic	9 May 2024
KII9	Taiwan	Journalist and representative of a media NGO	10 May 2024
KII10	Vietnam	Representative of a diaspora NGO	13 May 2024
KII11	Sri Lanka	Representative of an organisation working on digital rights	16 May 2024
KII12	Pakistan	Representative of an organisation working on digital rights	5 August 2024
KII13	Cambodia	Representative of an organisation working on digital rights	13 August 2024

ASIACENTRE

Asia Centre is a civil society research institute with Special Consultative Status with the United Nations Economic and Social Council (UN ECOSOC).

The Centre's core activities involve research, capacity-building, advocacy and media initiatives, having its programmatic priority on four key constitutional liberties as enshrined in the Universal Declaration on Human Rights (UDHR): freedom of religion or belief (Article 18), freedom of expression (Article 19), freedom of association (Article 20) and the right to political participation (Article 21).

Asia Centre collaborates with civil society stakeholders, international non-governmental organisations (INGOs), and duty-bearers to support their respective initiatives.

It operates from its Research Hub and Meeting Hub in Bangkok (Thailand), Media Hub in Johor Bahru (Malaysia), and Training Hub in Phnom Penh (Cambodia).

Asia Centre
Asia Centre
Asia Centre
@asiacentre_org
asiacentre_org
asiacentre

website: asiacentre.org
email: contact@asiacentre.org